НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО

Факультет інформатики та обчислювальної техніки
(назва факультету, інституту)

Кафедра автоматизованих систем обробки інформації і управління
(назва кафедри)

"На правах рукопису"
УДК *621.391*

«До захисту допущено»
Завідувач кафедри

_____ О.А.Павлов
(підпис) (ініціали, прізвище)

“ ” _____ 20 *18* р.

МАГІСТЕРСЬКА ДИСЕРТАЦІЯ

на здобуття ступеня магістра

за спеціальністю *122 Комп'ютерні науки та інформаційні технології*
(код та назва спеціальності)

спеціалізацією *Інформаційні управляючі системи та технології*
(код та назва спеціалізації)

на тему: *Методи комп’ютерної стеганографії для аудіо контейнерів*

Виконав: студент *VI* курсу групи ІС-63м
(шифр групи)

Поліщук Андрій Олександрович _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник *проф., д.ф.-м.н., проф. Задірака В. К.* _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант *к.т.н., доц. Жданова О.Г.* _____
(науковий ступінь, вчене звання, прізвище, ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018

РЕФЕРАТ

Магістерська дисертація: 101с., 23 рис., 10 табл., 1 додаток, 69 джерел.

Актуальність. Комп'ютерна стеганографія розвивається доволі інтенсивно, застосовуються відомі і розробляються нові методи стеганографії, засновані на різноманітних областях науки. Стеганографічні системи переходять в нову фазу свого розвитку, сьогодні вже велика їх частина при приховуванні інформації враховує характеристики і природу стеганоконтейнерів, що зберігає дані.

Комп'ютерна стеганографія знайшла своє застосування в багатьох областях людської діяльності:

- таємна передача конфіденційної інформації в мультимедійних файлах;
- захист авторських прав на аудіо- та відеоматеріали в електронному вигляді;
- створення таємних архівів;
- подолання систем моніторингу та управління мережевими ресурсами;
- камуфлювання програмного забезпечення;
- обслуговування політичної, технічної, військової та інших видів розвідки.

При передачі конфіденційного повідомлення, вкрапленого в аудіо контейнер, необхідно мінімізувати спотворення контейнеру, задля безпеки цієї передачі. Таким чином, розробка ефективних методів захисту цифрової інформації, зокрема методів комп’ютерної стеганографії та стеганоаналізу, вкрапленої в різноманітні контейнери, актуальні та мають важливе значення.

Зв’язок роботи з науковими програмами, планами, темами. Робота виконана на філії кафедри автоматизованих систем обробки інформації та управління в Інституті кібернетики ім. В.М. Глушкова НАН України в рамках науково-дослідної теми «Розробити оптимальні за точністю та швидкодією алгоритми розв’язання задач: інтегрування швидкоосцилюючих функцій, цифрової обробки сигналів та зображень, дистанційного моніторингу об’єктів, інформаційної безпеки» (номер державної реєстрації: 0114U000357).

Мета дослідження – розробка модифікації алгоритму, на базі існуючого, з метою мінімізації помітних змін вхідних об’єктів.

Для досягнення мети необхідно виконати наступні **завдання**:

- охарактеризувати наявні методи стеганографії аудіо контейнерів;
- визначити та проаналізувати недоліки наявних методів;
- провести модифікації існуючих алгоритмів;
- запропонувати модифікацію методу з вищою стеганостійкістю системи;
- визначити ефективність створеного рішення.

Об’єкт дослідження – процес захисту інформації, вкрапленої в аудіо контейнер, з мінімізацією його помітних змін.

Предмет дослідження – методи та алгоритми комп’ютерної стеганографії і стеганоаналізу для аудіо контейнерів.

Методи дослідження, застосовані у даній роботі, базуються на методах комп’ютерної стеганографії.

Наукова новизна одержаних результатів полягає у використанні існуючих ефективних стеганографічних алгоритмів з порівнянням результатів, з точки зору стеганостійкості. Пропозиції щодо підвищення стеганостійкості цих алгоритмів.

Публікації. Матеріали роботи представлено у двох наукових статтях на міжнародних конференціях ISCIENCE 2017 та ISCIENCE 2018, Переяслав-Хмельницький, Україна.

ЗАХИСТ ІНФОРМАЦІЇ, СТЕГАНОГРАФІЯ, СТЕГАНОАНАЛІЗ, СТЕГАНОКОНТЕЙНЕР, АУДІО КОНТЕЙНЕР, ВКРАПЛЕННЯ ІНФОРМАЦІЇ

ABSTRACT

Master dissertation: 101 p., 23 pic., 10 tabl., 1 Add., 69 ref.

Actuality. Computer steganography develops quite intensively, known and developed new methods of steganography, based on various fields of science. The steganographic systems are moving into a new phase of their development, today their large part in concealing the information takes into account the characteristics and nature of the stacking containers that store the data.

Computer steganography has found its application in many areas of human activity:

- secret transmission of confidential information in multimedia files;
- copyright protection of audio and video materials in electronic form;
- creation of secret archives;
- overcoming of monitoring and management systems of network resources;
- camouflage of the software;
- maintenance of political, technical, military and other types of intelligence.

When sending a confidential message embedded in an audio container, it is necessary to minimize the distortion of the container, for the safety of this transmission. Thus, the development of effective methods for the protection of digital information, in particular the methods of computer steganography and steganoanalysis, interspersed in a variety of containers, are relevant and important.

Connection with academic papers, plans, themes. The work was performed at the department of the automated systems of information processing and management at the Institute of Cybernetics named after. VM Glushkov of the National Academy of Sciences of Ukraine within the framework of the research theme "To develop algorithms optimal for accuracy and speed of solving problems: integration of fast-sensing functions, digital processing of signals and images, remote monitoring of objects, information security" (state registration: 0114U000357).

The goal of the research is to develop a modification of an algorithm, based on existing, in order to minimize significant changes in input objects.

To achieve the goal, you must accomplish the following **tasks**:

- characterize the existing methods of steganography of audio containers;
- identify and analyze the disadvantages of existing methods;
- to modify existing algorithms;
- to offer a modification of an existing method with a higher quadraticity of the system;
- determine the effectiveness of the solution.

The object of the research - the process of protecting information, embedded in the audio container, minimizing its noticeable changes.

Subject of the research - methods and algorithms of computer steganography and steganoanalysis for audio containers.

The research methods used in this paper are based on the methods of computer steganography.

The scientific novelty of the obtained results is to use existing effective steganographic algorithms with comparison of results, in terms of quilting resistance. Proposals to improve the queuing performance of these algorithms.

Publications. The materials of the work were presented in two scientific articles at the international conferences ISCIENCE 2017 and ISCIENCE 2018, PereyaslavKhmelnitsky, Ukraine.

PROTECTION OF INFORMATION, STEGANOGRAPHY, STEGANOANALIZE, STEGANOCONTREASER, AUDIO CONTAINER, DISTRIBUTION OF INFORMATION

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ

AWGN – англ. Additive white Gaussian noise – адитивний гауссовий білий шум.

LSB – англ. Least Significant Bit – найменш значущий біт.

ССЛ – слухова система людини.

WAV – WAVE – формат файла-контейнера для зберігання записів оцифрованого аудіопотоку.

PSNR – англ. Peak signal-to-noise ratio – коефіцієнт пікового сигналу до шумового співвідношення

MSE – англ. Mean squared error – середньо-квадратична похибка.

ВСТУП

У сучасному інформаційному суспільстві велика кількість послуг забезпечується за допомогою комп’ютерних мереж та інформаційних технологій. Інформація, що представлена в цифровому вигляді, має бути надійно захищена від багатьох загроз: несанкціонованого доступу та використання, знищення, підробки, витоку, порушення ліцензійних угод, відмови від авторства та ін. Захист інформації є вкрай важливим як в комерційній, так і в державній сферах. Законом України "Про основи національної безпеки України" від 19.06.2003р. серед загроз національним інтересам і безпеці України в інформаційній сфері зазначені: комп'ютерні тероризм та злочинність; розголошення таємної чи конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; маніпулювання суспільною свідомістю, зокрема, шляхом поширення недостовірної інформації. Таким чином, питання розроблення ефективних методів захисту цифрової інформації, зокрема методів комп’ютерної стеганографії та стеганоаналізу, актуальні та мають важливе значення для держави й суспільства.

Найбільшого розвитку в Україні та світі здобула така наука про методи забезпечення конфіденційності та автентичності інформації, як криптографія. Разом з тим альтернативний захист може бути створений на базі стеганографії, а в певних застосуваннях і шляхом використання криптостеганографічних модулів. Крім того існують важливі задачі інформаційної безпеки, що є нерозв’язними виключно криптографічними методами, і зокрема, вони мають місце тоді, коли потрібно приховати факт існування конфіденційної інформації. Стеганографічні методи за своєю природою забезпечують більш високий рівень захисту, оскільки дані, що захищаються, та відповідно, факт їх передачі залишаються поза зоною уваги неуповноважених осіб.

Сучасні комп’ютерні технології обробки даних істотно підвищили рівень інформаційної безпеки завдяки глибокій інтеграції криптографічних засобів в інформаційні системи. Як відомо, на відміну від криптографічного захисту

інформації стеганографічні програмні засоби намагаються насамперед приховати сам факт існування конфіденційної інформації. Стеганографічні методи, які приховують інформацію у потоках оцифрованих сигналів та реалізуються на основі комп’ютерної техніки і програмного забезпечення, становлять предмет вивчення цифрової стеганографії. Актуальність дослідження методів стеганографії невпинно зростає, адже з поширенням персональних комп’ютерів, і особливо Інтернету, можливість конфіденційно передавати інформацію привертає увагу великої кількості людей. Переважна більшість теоретичних та практичних досліджень у галузі стеганографії присвячена саме розробці нових та вдосконаленню існуючих методів приховування даних.

Зростаючі можливості сучасних засобів зв'язку вимагають розробки спеціальних засобів безпечного зберігання та передачі інформації. Мережева безпека стає все більш актуальною з огляду зростаючих обсягів даних, що пересилаються по локальних і глобальних мережах. Для захисту інформації від несанкціонованого доступу та використання необхідно забезпечити конфіденційність і цілісність даних. Захисті інформації може бути забезпечено криптографією, стеганографією, або одночасно криптографією і стеганографією. При використанні криптографії інформація модифікується, перетворюється. В результаті перетворень приховується зміст повідомлення. Стеганографія, в свою чергу, приховує сам факт передачі або зберігання інформації. Це досягається шляхом впровадження інформації, що захищається, в різні мультимедійні об'єкти (контейнери), які не втрачають від цього своїх споживчих властивостей. Відносно обчислювальної техніки виділився окремий напрямок стеганографії - комп'ютерна стеганографія. Як контейнери тут використовуються файли різних форматів, мережеві пакети і т.д. Наприклад, інформацію можна впровадити в звуковий сигнал, який згодом відтворюється практично точно так (з тією ж якістю), як вхідний сигнал без впровадження.

З іншого боку, приховування даних можна використовувати в не комерційному секторі, щоб приховати інформацію, яку хтось хоче зберігати в

секреті. Стеганографія стала доступна для більшості користувачів і може застосовуватися в протизаконних цілях, наприклад, для несанкціонованої передачі комерційних або державних секретів; переписки терористичних угруповань. Тому з'являється необхідність у розробці ефективних методів виявлення прихованих вкладень, в мультимедійних об'єктах, переданих в комп'ютерних мережах.

Комп'ютерні технології надали нового імпульсу розвитку стеганографії, з'явилася комп'ютерна стеганографія, яка забезпечила непомітне, з позицій споживчих якостей, вбудовування даних в файли-контейнери, що містять в цифровому вигляді звуку або зображення.

Інтерес до цієї області залишається на високому рівні, хоча вже існує багато застосувань стеганографії на практиці. Прикладами таких застосувань є:

- захист інформації від несанкціонованого доступу;
- протидія системам моніторингу та керування ресурсами мереж;
- маскування програмного забезпечення від незареєстрованих користувачів;
- захист авторського права на деякі види інтелектуальної власності[2].

Проте, поточне покоління стеганографії аудіо контейнерів вимагає подальшого удосконалення. Ці поліпшення включають в себе ефективні методи для поліпшення стеганографічної стійкості стеганоконтейнерів.

1 Огляд стеганографії

1.1 Історія стеганографії

Щоб зрозуміти поняття стеганографії, ми повинні спочатку зрозуміти його попередника – криптографію. Криптографія - це мистецтво захисту інформації, перетворюючи його в незрозумілийя для читача формат, який називається шифрованим текстом. Щоб розшифрувати цей непрочитаний формат, потрібен секретний ключ. Криптографія спостерігається за людиною впродовж багатьох етапів еволюції.

Криптографію можна знайти ще у 1900 роках до н.е. в давньоєгипетському довіднику, де використовувались нестандартні ієрогліфи. Від 500 до 600 років до н.е. єврейські книжники використовували зворотний алфавіт з простим шифром. Від 50 до 60 років до н.е. Юлій Цезар використовував просту підміну з нормальним алфавітом у державних комунікаціях. Криптографія пройшла через історію зрізними варіаціями. Сьогодні криптографія досягла нового рівня, квантової криптографії. Квантова криптографія об'єднує фізику та криптографію для створення нової криптосистеми, яку неможливо перемогти без відправника та одержувача. Через довгу історію криптографії, стеганографія була розроблена сама по собі.

Стеганографія походить від грецького стегано (покрите або таємне) і -графію (написання або малюнок). Стеганографія може бути визначена як приховування інформації шляхом вставки повідомлень в інші, начебто звичайні повідомлення, графіки чи звуки. Перша стеганографічна техніка була розроблена в Стародавній Греції близько 440 року до н.е. Грецький правитель використовував ранню версію стеганографії, яка включала в себе: гоління голови раба, татуювання повідомлення на шкірі голови, очікування зрозростання волосся і відправлення раба на його шлях, щоб доставити повідомлення. Одержувач матиме голову раба, щоб розкрити повідомлення. Одержувач відповість у тій самій формі стеганографії. У той же період часу використовувався ще один ранній вид стеганографії. Цей метод включав Демерстуса, який написав повідомлення спартанцям про попередження вигадливих вторгнень з Ксеркса. Повідомлення було вирізано на дереві, а потім накрито свіжим

шаром воску. Ця, здавалося б, порожня таблетка була успішно доставлена з прихованим повідомленням. Стеганографія продовжувала розвиватися на початку 1600-х років, оскільки сер Френсіс Бейкон використовував варіацію в обличчї типу, щоб нести кожен біт кодування.

Стеганографія продовжує з часом розвиватися на нових рівнях. Під час війни стеганографія також широко використовувалась. Під час американської революційної війни британські та американські сили використовували різні види невидимих чорнил. Невидиме чорнило включає в себе поширені джерела, до яких належить молоко, оцет, фруктовий сік та сеча. Щоб розшифрувати ці приховані повідомлення, потрібно світло або тепло. Під час Другої світової війни німці представили мікрододатки. Мікрододатки – це звичайні документи, фотографії та плани зменшені у розмірі до розміру періоду та прикріплені до звичайних документів. Нульові шифри також використовувалися для передачі секретних повідомлень. Нульові шифри - незашифровані повідомлення з реальними повідомленнями, вбудованими в поточний текст. Приховані повідомлення були важко інтерпретувати всередині звичайних повідомлень.

1.2 Поняття стеганографії

Стеганографія – це мистецтво приховування секретної інформації в файлі таким чином, що тільки відправник та отримувач можуть знати про її наявність. Конфіденційна інформація закодована так, що сам факт існування повідомлення приховується.

У порівнянні з досить добре дослідженими криптографічними системами, поняття і оцінки безпеки стеганографічних систем більш складні і мають багатогранні тлумачення. Зокрема, це пояснюється як недостатньою теоретичної та практичної опрацюванням питань безпеки стегосистем, так і великою різноманітністю завдань стеганографічного захисту інформації[29].

Можна сказати, що стеганографія – це один із шляхів підтримки інформаційної безпеки. Вона являє собою метод організації зв’язку, який приховує сам факт наявності таємних повідомлень. Стеганографічні методи активно

використовуються для захисту інформації від сторонніх користувачів та для маскування програмного забезпечення[25].

На конференції Information Hiding (First Information Workschop) у 1996 році були обговорені всі базові поняття стеганографії та прийнята єдина термінологія[3,4]. Згідно з цією термінологією стеганографічна система або стегосистема – це сукупність засобів та методів, які використовуються для формулювання таємного каналу зв'язку. Будь-яка інформація, в якій приховані таємні дані, називається контейнером. За контейнер може слугувати будь-який файл чи потік даних. Контейнер, який не містить таємного повідомлення, називають порожнім, а той, що містить – заповненим або стегоконтейнером. Канал передачі сгегоконтейнера має назву стеганографічного каналу або стегоканалу. Таємний ключ, який необхідний для «вкраплення» інформації в контейнер, називається стегоключем або просто ключем. Залежно від кількості рівнів захисту в стегосистемі може використовуватись як один, так і декілька ключів[16].

Визначення 1.1. Стеганографічна система (стеганосистема) – це сукупність $\Sigma = (X, M, K, Y, E, D)$ пустих контейнерів X, повідомлень M, ключів K, заповнених контейнерів Y і перетворень E та D, що їх пов'язують (алгоритмів вкраплення та вилучення).

Визначення 1.2. Контейнер (носій) – це нетаємна інформація, в якій будуть приховані конфіденційні дані (повідомлення). В комп'ютерній стеганографії контейнером може слугувати будь-який файл чи потік даних. В силу своєї надлишковості найчастіше цифровими контейнерами виступають зображення, аудіо чи відеосигнали.

Визначення 1.3. Повідомленням називається таємна інформація, наявність якої необхідно приховати.

Визначення 1.4. Стеганоключ – елемент стеганосистеми, який параметризує алгоритми вкраплення й вилучення, та відомий тільки відправнику і одержувачу стеганоконтейнера. Стеганоключ зокрема може визначати область вкраплення (часова/просторова чи частотна), базис частотного розкладу, правила розбиття

контейнера на сегменти, силу вкраплення, індекси задіяних коефіцієнтів, точки квантування, кодову книгу, вектор розширення та інше.

Визначення 1.5. Пустим називають контейнер, який не містить прихованого стеганографічними методами повідомлення.

Визначення 1.6. Контейнер, що містить приховану інформацію, називають заповненим або стеганоконтейнером, або стеганограмою.

Задача стеганографічної системи – розмістити вхідне повідомлення в контейнері таким чином, щоб будь-яка стороння людина не змогла помітити нічого, крім його основною вмісту. Основний вміст контейнера не відіграє ніякої ролі ні для відправника, ні для одержувача, яких цікавить лише успішна передача повідомлення, вміщеного в ньому (стеганограми). Потрібно обов'язково враховувати те, що сам факт відправлення контейнера від автора до одержувача не повинен виглядати дивним, а також не повинно спостерігатись помітних відхилень контейнера від норми.

Схематично узагальнена модель стеганографічної системи представлена на рисунку 2.1.

Рисунок 2.1 – Узагальнена модель стеганографічної системи

За аналогією з криптографією, якщо при вкрапленні та вилученні повідомлення використовується один і той же ключ – стеганосистема вважається симетричною, якщо різні – асиметричною.

Стеганографія, як наука, інтегрує в собі здобутки криптографії, теорії інформації, теорії ймовірності та математичної статистики, теорії дискретних ортогональних перетворень, цифрової обробки сигналів та зображень, розпізнавання образів та ін. Зауважимо, що існує підхід, згідно якому стеганографічні системи розглядаються як узагальнення криптографічних. Стеганографічні методи володіють унікальними властивостями, що робить їх незамінними при вирішенні певних задач захисту.

Комп'ютерна стеганографія розвивається у декількох напрямах, що мають як багато спільних рис, так і певні характерні відмінності, спричинені особливостями практичного застосування. Так, серед стеганосистем виділяють системи прихованої передачі даних, цифрових водяних знаків, ідентифікаційних номерів («відбитків пальців») та заголовків [1]. Задача будь-якої стеганографічної системи – розмістити певне повідомлення в контейнері таким чином, щоб будь-яка стороння людина не змогла помітити різниці між модифікованим контейнером та оригінальним. Зазвичай стеганосистема будується так, щоб забезпечити заданий компроміс її основних характеристик, таких як непомітність, стійкість, безпека, пропускна здатність, обчислювальна складність. Розглянемо особливості кожного з виділених видів стеганосистем [2].

Системи прихованої передачі даних застосовуються для організації таємної комунікації. Вони відрізняються від усіх інших тим, що в цьому випадку оригінальний вміст контейнера не грає ніякої ролі ні для відправника, ні для одержувача, яких цікавить лише успішна передача вкрапленого повідомлення. Разом із тим потрібно обов'язково враховувати, що факт відправлення контейнера від відправника до одержувача не повинен виглядати дивним, а також не повинно спостерігатися помітних відхилень контейнера від норми. Основна мета таких систем – приховати наявність стеганоканалу, унеможливити розрізнення пустих і заповнених контейнерів без знання ключа. Для таких систем звичайно вважається, що контейнер не підлягає спотворенням в процесі його передачі по каналу зв'язку ($Y' = Y$), тому що таємна комунікація відбувається через відкритий канал цифрової

мережі, наприклад, інтернет, що забезпечує відсутність спотворень інформації при її передачі.

Як згадувалось раніше, комп'ютерна стеганографія знайшла своє застосування в багатьох областях людської діяльності: таємна передача конфіденційної інформації в мультимедійних файлах; захист авторських прав на аудіо- та відеоматеріали в електронному вигляді; створення таємних архівів; подолання систем моніторингу та управління мережевими ресурсами; камуфлювання програмного забезпечення; обслуговування політичної, технічної, військової та інших видів розвідки[6].

1.3 Актуальність стеганографії

Щодо актуальності стеганографії в теперішній час, можна сказати, що комп'ютерна стеганографія розвивається доволі інтенсивно, застосовуються відомі і розробляються нові методи стеганографії, засновані на різноманітних областях науки. Стеганографічні системи переходять в нову фазу свого розвитку, сьогодні вже велика їх частина при приховуванні інформації враховує характеристики і природу стегоконтейнеру, що зберігає дані[20].

Таким чином, до теперішнього часу для цілого кола фахівців з'явилася необхідність ознайомлення з основами сучасної комп'ютерної стеганографії, завданням яких є не тільки розробка, аналіз або протидія засобам стеганографії, а й кваліфікований вибір існуючих засобів і їх вміле використання для вирішення конкретних прикладних завдань захисту інформації.

Зупинимося дещо докладніше на кожній із задач стеганографії. В першу задачу входить прихована передача викраденої інформації. Стеганографічні методи, спрямовані на протидію системам моніторингу та управління мережевими ресурсами, можуть застосовуватися в тих регіонах світу, де регулюється або забороняється використання стійких криптографічних методів. Стеганографічні методи покликані протистояти спробам контролю над інформаційним простором при проходженні інформації через сервери управління локальних і глобальних обчислювальних мереж[50].

Іншим важливим завданням стеганографії є камуфлювання програмного забезпечення. У тих випадках, коли використання програмного забезпечення є небажаним, воно може бути закамуфльоване під стандартні універсальні програмні продукти (наприклад, текстові редактори) або приховано в файлах мультимедіа (наприклад, в звуковому супроводі комп'ютерних ігор). Зауважимо, що інформація не передається від однієї особи іншій, а залишається на магнітному диску. В цьому випадку стеганографічні методи дозволяють приховувати не факт передачі, а факт існування інформації[9].

При обробці медичних зображень (рентгенівських знімків, результатів ЕКГ, тощо) необхідним є зв'язок самого зображення і даних про пацієнта (П.І.Б., дата, лікуючий лікар). Використання методів впровадження характеризує інформацію про пацієнта в графічний файл, що дозволяє не тільки усунути випадкову або навмисну підміну і втрату медичних висновків, але і дозволяє автоматично обробляти і зберігати результати на ЕОМ. Крім того, медична безпека досліджує способи психофізичного впливу на людину (наприклад, використання 25-го кадру) і заходи захисту від них[24].

Ще однією областю використання стеганографії є захист авторського права від піратства. На комп'ютерні графічні зображення наноситься спеціальна мітка, яка залишається невидимою для очей, але розпізнається спеціальним програмним забезпеченням. Таке забезпечення вже використовується в комп'ютерних версіях деяких журналів. Цей напрямок стеганографії призначений не тільки для обробки зображень, а й для файлів з аудіо та відео і призначений для забезпечення захисту інтелектуальної власності. Захист інтелектуальної власності включає впровадження водяних знаків і зняття відбитків пальців, які дозволяють довести незаконність використання авторського права. Водяні знаки – це мітки авторського права, зірвані в змісті. Відбитки пальців - це мітки, вкладені в копії об'єкта, які визначаються для різних замовників (подібно прихованого реєстраційного номеру). Це дозволяє власнику інтелектуальної власності ідентифікувати замовників та визначати тих, хто порушив ліцензійну угоду[21].

Існує певна різниця між класичним формулюванням стеганографічної проблеми, відомої як «Проблема ув'язнених», і проблемою захисту авторських прав. В першій проблемі успішна атака на систему полягає у виявленні факту приховування, у другому - навпаки, всім може бути відомо про наявність впроваджених міток, так що успішна атака на систему полягає не у виявленні міток, а в їх видаленні або внесення більше позначок. Запобігання таких методів злому системи приховування може ґрунтуватися на впровадженні цифрової сигнатури об'єкта або тимчасових міток. Збільшення обсягів баз даних, що містять відео і аудіо продукцію, вимагає ефективної системи пошуку та ідентифікації змісту файлу. З цією метою в мультимедійні дані впроваджується інформація про автора твору, виконавця, зміст, дату, тощо[22].

Ще один напрямок стеганографії - можливість правдоподібного заперечення, заснований на стеганографічній файловій системі. Стеганографічна система файлів є механізмом захисту, здатним забезпечити високу ступінь захисту від вимушеного розголошення інформації. Цей механізм дозволяє правдоподібним чином заперечувати існування окремих файлів. Навіть якщо зловмисник має повний доступ до ресурсів системи.

Методи стеганографії використовуються для автоматичного контролю реклами, що передається по радіо - це автоматизовані системи, призначені для перевірки факту відтворення рекламного повідомлення згідно з укладеним договором.

1.4 Ризики та загрози використання стеганографії

Великі корпорації все більше усвідомлюють ризики, пов'язані із використанням стеганографії. З брандмауерами, системи виявлення вторгнень та іншими відповідними засобами захисту, які ще не в змозі виявити повідомлення, сховані в файлі, хакери здатні виконувати такі завдання, як створення креслень для проникнення в комп'ютерні системи компанії, а саме в аудіофайли, що зберігаються на власній веб-сторінці фірми[32].

В усьому світі уряди прагнуть забезпечити, отримання ключів шифрування для читання повідомлень, коли вони викликають підозру, що такі злочинці, як

контрабандисти наркотиків, відмивачі коштів чи терористи, використовують зашифровані повідомлення. Як наслідок, ті, хто зловмисним наміром не використовують метод спілкування, можуть бути легко перехоплені і прочитані.

Пошук в Інтернеті відкриє сотні тисяч посилань на сторінки зі стеганографією. Посилання включають посилання на безкоштовне завантажуване програмне забезпечення та математичні формули описуючи, як працює ця техніка. Злочинці будь-якого типу намагаються приховувати дані щодня, а в Інтернеті є можливість це робити. Коли приховування секретних даних використовується для зловмисних цілей, ця техніка спілкування стає загрозою для безпеки всесвітньої інформаційної інфраструктури[25].

Стеганографія створює ризики, для національної безпеки. Хоча стеганографія, як видається, є гарним способом безпечного обміну конфіденційною інформацією, її можна також неправильно використовувати. Існують спекуляції про те, що терористи використовують ці методи для спілкування через Інтернет, здавалося б, невинні веб-сайти. Теорія полягає в тому, що терористичні групи, як стверджується, приховують карти та фотографії терористичних цілей та розміщують інструкції щодо терористичної діяльності в спортивних чатах, порнографічних плакатах та інших веб-сайтах. Фактично незабаром після 11 вересня 2001 року було проведено розслідування про сканування більше двох мільйонів зображень з веб-сайту eBay для прихованих повідомлень, що містяться в них. Нібито нічого не знайдено, але уряд, безсумнівно, побачив ризик[61].

Загроза, викликана стеганографією, дуже реальна. Її використання нелегко виявити або перехопити, оскільки інформація не повинна транслюватися через Інтернет. Приховане повідомлення може зберігатись без нагляду на веб-сайті, і його можна переглядати з усього світу. Незважаючи на те, що головна загроза на даний момент полягає у забезпеченні національної безпеки, ця технологія безсумнівно використовується і для інших аморальних цілей. Тому, хоч стеганографія ще не є такою загрозою, але IT-аудитори борються проти неї. Це той випадок, який необхідно розглянути та зрозуміти для можливих майбутніх подій[45].

Не всі випадки використання стеганографії є поганими. Водяні знаки можуть бути вставлені для посвідчення особи, що ускладнює підробку для того, хто намагається зробити копію. Іншим позитивним чинником є те, що абсолютно-правова чи конфіденційна інформація може бути передана більш надійно. Крім того, компанії використовують техніку, щоб робити повсякденний бізнес більш безпечним. Наприклад, корпорація Digimarc, провідний постачальник захищених медіа-рішень, надає безпечні рішення щодо ідентифікації водяних знаків урядам у всьому світі.

1.5 Види стеганографічних методів

Залежно від виду спеціальних властивостей форматів розрізняють такі стеганографічні методи:

- засновані на використанні зарезервованих для розширення полів комп'ютерних форматів файлів. Поля для розширення є в багатьох мультимедійних форматах і призначені для вдосконалення, оновлення і сумісності нових версій форматів зі старими. Як правило, ці поля заповнюються нульовою інформацією і не враховуються програмами, і тому можуть бути використані для передачі додаткової інформації. Недоліком цих методів є низький ступінь скритності і передача невеликих обсягів інформації, що приховується[64].
- Засновані на спеціальному форматуванні текстових файлів, відомі вже давно, використовувалися задовго до появи комп'ютерних технологій і включають в себе методи[14]:
  - використовують заздалегідь відоме зміщення слів, речень, абзаців в текстовому файлі, засновані на зміні положення рядків і розстановки слів в реченні, що виробляється вставкою додаткових пробілів між словами, збільшень проміжків непомітно візуально, але фактично передає приховану інформацію;
  - засновані на виборі певних позицій букв (нульовий шифр). Наприклад, вибір п'ятої літери кожного останнього слова в рядку в межах однієї сторінки. Сюди ж відносяться художні прийоми тайнопису - акростих,

добре відомий знавцям поезії, це така організація віршованого тексту, при якій, наприклад, початкові літери кожного рядки утворюють приховуване повідомлення[67];

- використовують спеціальні властивості полів форматів, які не відображаються на екрані. Наприклад, використання чорного шрифту на чорному тлі спеціальних «невидимих», прихованих полів для організації виносок і посилань[17].

– Засновані на приховуванні в невикористовуваних місцях гнучких дисків. Назва цієї групи говорить сама за себе і має ті ж переваги і недоліки, що і методи, засновані на використанні зарезервованих для розширення полів форматів.
– Засновані на імітуючій функції (мнемосхема-функція) - цей вид стеганографії заснований на генерації текстів і є узагальненням акровірша. Для заданого приховуваного повідомлення генерується осмислений текст, який містить приховуване повідомлення. При цьому текст є граматично і синтаксично правильним і статистично еквівалентним до текстів на подібну тему. Такі тексти можуть не бути підозрілими для систем моніторингу мережі, але все ж людина може швидко визначити відсутність будь-якого сенсу в змісті тексту[28].
– Засновані на використанні кодів, що виправляють помилки; приховування даних в додатковій інформації, використовуваної перешкодозахищеними кодами при виправленні випадкових помилок і забезпеченні точності передачі цифрового інформації. Якщо інформація захована, а на стороні прицмача код знятий, то спостерігач не буде навіть знати, що було відправлено повідомлення.
– Засновані на видаленні заголовка файлу. У цьому методі приховуване повідомлення шифрується і у результаті видаляється ідентифікація заголовку, залишаючи тільки шифровані дані, які видаються за випадкові, можливо, як спотворена інформація. Одержувач заздалегідь знає про передачу секретних даних і має недостатньо інформації. При цьому проблема приховування

вирішується тільки частково. Цей метод не є повністю стеганографічним методом, а служить скоріше доповненням до них, хоча багато програмні засоби (White Noise Storm) забезпечують цю додаткову ступінь захисту з використанням алгоритму шифрування PGP[18].

Це лише деякі методи, що ілюструють евристичний підхід в стеганографії. Недоліками відомих методів, заснованих на використанні спеціальних властивостей форматів файлів, є:

- низький ступінь скритності (скритність грунтується на незнанні противником самого алгоритму приховування);
- передача невеликих обсягів інформації, що приховується.

До переваг можна віднести простоту реалізації. Слід зауважити, що вже опубліковано ряд програм, що реалізують деякі алгоритми[5,19].

1.6 Стислий огляд методів стеганографії

Розглянемо більш детально декілька методів. Одним з найбільш поширених методів є LSB (Least Significant Bit, найменш значущий біт) алгоритм, який замінює найменший значущий біт в декількох байтах файлу-носія, щоб приховати послідовність байтів, що містять приховані дані. Це, як правило, ефективно тоді, коли заміна молодшого біта не тягне за собою значне погіршення якості.

Для простоти опису можна розглянути принцип роботи цього методу на прикладі 24-бітного реєстрового RGB-зображення. Одна точка зображення в цьому форматі кодується трьома байтами, кожен з яких відповідає за інтенсивність одного з трьох складових картинки[34].

В результаті зміщення кольорів з червоного, зеленого і синього каналів, піксель отримує потрібний відтінок. Щоб наочніше побачити принцип дії методу LSB, розглянемо детальніше кожен з трьох байтів в бітовому вигляді. Молодші розряди в меншій мірі впливають на підсумкове зображення, ніж старші. З цього можна зробити висновок, що заміна одного або двох молодших, найменш значущих бітів, на інші довільні біти настільки незначно спотворить відтінок пікселя, що глядач просто не помітить зміни. Припустимо, нам потрібно приховати в даній

точці зображення шість біт: 101100. Для цього розіб'ємо їх на три пари і замінимо ними по два молодших біта в кожному каналі[53].

В результаті ми отримаємо новий відтінок, дуже схожий на вихідний. Ці кольори важко розрізнити навіть на великий за площею заливці. Як показує практика, заміна двох молодших бітів не сприймається людським оком. У разі необхідності можна зайняти і три розряди, що досить незначно позначиться на картинці. Тепер можна порахувати корисний об'єм такого RGB-контейнера. Займаючи два біта з восьми на кожен канал, ми будемо мати можливість заховати три байта корисної інформації на кожні чотири пікселя зображення, що відповідає 25% обсягу картинки. Таким чином, маючи файл зображення розміром 200 Кбайт, ми можемо приховати в ньому до 50 Кбайт довільних даних так, що неозброєним оком ці зміни не будуть помітні[13,15].

Всі контейнери потрібно розділити на два класи: «чисті» і «зашумлені». У «чистих» контейнерах простежується зв'язок між молодшим бітом, який піддається змінам, і іншими бітами елементів, а також видно залежність самих молодших бітів між собою. Впровадження повідомлення в «чистий» контейнер руйнує існуючі залежності, що дуже легко виявляється спостерігачем. Якщо ж контейнер «зашумлений», то визначити вкладення стає набагато складніше. Таким чином, в якості файлів-контейнерів для методу LSB рекомендується використовувати файли, які не були створені на цьому комп'ютері [23].

Метод LSB має і переваги, і недоліки. До переваг можна віднести:

- розмір файлу-контейнеру залишається незмінним;
- при заміні одного біту, неможливо виявити зміни;
- можливість змінювати пропускну здатність, змінюючи кількість біт, які замінюються.

Недоліком даного методу є нестійкість до всіх видів атак. Тобто, алгоритм можна використати тільки при відсутності шуму в каналі передачі даних.

Розглянемо ще один метод, парне кодування, який є одним з найнадійніших способів аудіо стеганографії. Замість того, щоб розбивати сигнал в окремих вибірках, цей метод розбиває сигнал на окремі частини і вбудовує кожен біт

секретного повідомлення в парний біт. Якщо парний біт в обраній області не підлягає кодуванню в секретний біт, то процес інвертує молодший біт однієї з вибірки даної області[13].

Також, можна використовувати метод фазового кодування. Його суть полягає у заміні фази вихідного звукового сегмента на опорну фазу, яка представляє собою секретну інформацію. Інші сегменти фази коригуються для збереження певної фази між сегментами. З точки зору відношення сигналу до шуму, фазове кодування є одним з найбільш ефективних методів кодування. Коли відбувається різка зміна фазового співвідношення між кожною частотною складовою, шуми стають помітними. Проте, якщо фазу модифікувати не сильно, то людське вухо не розпізнає будь-яких змін. Виходячи з цього можна сказати, що цей метод заснований на тому, що зміни, внесені в аудіо файл, будуть непомітні для людського слуху[7].

Фазове кодування включає в себе наступні кроки:

- розділити оригінальний звуковий сигнал на більш дрібні сегменти таким чином, щоб їх загальна довжина дорівнювала довжині повідомлення;
- створюється матриця фаз за допомогою дискретного перетворення Фур'є[26];
- обчислюється різниця фаз між сусідніми сегментами;
- у зв'язку з тим, що фазові зрушення між двома сусідніми сегментами можуть бути легко виявлені, в стегосигналі повинні бути збережені різниці фаз. Тому секретне повідомлення вбудовується тільки в фазу першого сегмента[10,11];
- використовуючи нову фазу першого сегмента створюється нова матриці фаз і різниці між ними;
- звуковий сигнал відновлюється шляхом застосування зворотного дискретного перетворення Фур'є з використанням нової матриці і вихідної матриці величин, після чого звукові сегменти зчіплюються.

Одержувач повинен знати довжину сегмента, щоб отримати секретне повідомлення зі звукового файлу. Після чого одержувач за допомогою дискретного перетворення Фур'є може отримати секретну інформацію[27].

В аудіо стеганографії метод розширеного спектру намагається передати секретні відомості по спектру частот звукового сигналу. Цей метод чимось схожий з

вище описаним методом LSB, який передає біти повідомлення випадковим чином по всьому звуковому файлу. Проте, на відміну від способу LSB, метод розширеного спектру поширює секретну інформацію по спектру частот звукового файлу, використовуючи код, який не залежить від фактичного сигналу. В результаті кінцевий сигнал займає смугу пропускання, яка розміром більше, ніж необхідний розмір для передачі.

Метод розширеного спектра може зробити вагомий вклад в підвищення продуктивності в порівнянні з методами LSB, фазового та парного кодувань шляхом помірної швидкості передачі даних і високим рівнем стійкості. Однак, метод розширеного спектру має один істотний недолік - він може вносити шум в аудіо файл.

Метод-відлуння вбудовує секретну інформацію в звуковий файл, вводячи відлуння в дискретний сигнал. Головні переваги цього методу - це висока швидкість передачі даних, а також підвищена стійкість в порівнянні з іншими методами. Якщо з вихідного сигналу можна виділити тільки одне відлуння, то може бути закодований тільки один біт секретної інформації. Отже, перед початком процесу кодування вихідний сигнал розбивається на блоки. Після виконання кодування блоки об'єднуються разом, щоб утворити остаточний вихідний сигнал[39].

Висновки до розділу

Узагальнюючи, можемо зробити висновок, що основні недоліки використання таких методів як відлуння, розширеного спектру і парності кодування полягають в тому, що вони вносять шум в аудіо файл, який може бути досить помітним для людського вуха, а також надійність даних методів викликає питання. Щодо фазового кодування, то цей метод має основний недолік, що полягає в низькій швидкості передачі даних через те, що секретне повідомлення кодується тільки на першому сегменті сигналу. Отже, цей метод використовується тільки тоді, коли передається невелика кількість даних[12].

Серед вище запропонованих методів стеганографії метод найменшого значущого біта або LSB є найпростішим методом для вбудовування секретної інформації. Метод LSB дозволяє закодувати велику кількість даних в звуковий

файл, забезпечує більш високий рівень безпеки в порівнянні з іншими методами, є ефективним методом для приховування секретної інформації від зловмисників, а також гарантує незмінність розміру файлу навіть після кодування і підходить для будь-якого типу формату аудіо файлу[23].

Конкретна реалізація будь-якого перерахованого методу впровадження тісно пов’язана з фізичною природою сигналу-повідомлення та сигналу-контейнера. Найчастіше, в якості контейнера вибираються аудіо-сигнали і зображення. Для високоякісного відтворення аудіо-сигналів і зображень сучасна техніка використовує цифровий запис таких сигналів. В силу своєї аналогової природи, аудіо-сигнали та зображення містять надлишкову інформацію, яку легко замінити на певне повідомлення. При цьому бітовий склад стего відрізняється від бітового складу контейнера, і це не повинно виявлятися за допомогою людських органів чуття і надавати істотного впливу на роботу телекомунікаційної системи. Виключеннями є ряд методів впровадження цифрового водяного знака, де водяний знак виступає в ролі прихованого повідомлення і може бути помітним або накладати певні обмеження на редагування стего-контейнеру.

2 Властивості та методи стеганографії

2.1 Базові характеристики

Задача будь-якої стеганографічної системи – вкрапити повідомлення в контейнер таким чином, щоб будь-який сторонній спостерігач не зміг помітити різниці між оригінальним контейнером та модифікованим. Зазвичай система будується так щоб забезпечити певний компроміс її базових характеристик, до яких відносяться невідчутність, стійкість, безпека, пропускна здатність створюваного стеганоканалу та обчислювальна складність реалізації.

Невідчутність. Вкраплення повідомлення повинне зберігати перцепційну якість оригінального контейнера. Для аудіосигналів повідомлення повинне бути невідчутним, для зображень – візуально непомітним. Невідчутності повідомлення можна досягнути внесенням мінімальних модифікацій при стеганоперетворенні контейнера, наприклад, на рівні похибки квантування при оцифровці. Крім того, досягти невідчутності допомагає врахування властивостей систем людського слуху та зору. Так, людське вухо працює в режимі частотного аналізатору, що має інтегруючі властивості у межах критичних смуг слуху [64]. Воно здатне сприймати коливання від 20 до 20000 Гц, при цьому найбільш чутливе до звукових компонент з частотами від 500 до 6000 Гц. При розробленні аудіостеганометодів можуть бути використані такі особливості системи людського слуху [25]:

- модифікації, що вносяться в компоненти аудіосигналу, які лежать нижче абсолютного порогу чутності, невідчутні людині;
- поріг чутності одних звукових компонент змінюється в присутності інших: слабке, але чутне звукове коливання стає невідчутним при наявності більш гучного, тобто маскується ним;
- при сприйнятті аудіосигналів людиною крім частотного маскування відбувається також часове, яке ділять на післямаскування та передмаскування.

На практиці чисельними показниками невідчутності часто стають співвідношення сигнал/шум SNR, середньоквадратична похибка MSE, максимальна різниця MD та інші [16].

Стійкість. Суть поняття стійкості залежить від типу атак, які характерні для тієї чи іншої стеганографічної системи. Так, для систем прихованої передачі даних найбільш характерними є пасивні атаки, тому у цьому випадку під стійкою насамперед розуміють систему, яка здатна ефективно їм протидіяти[31].

Для інших видів стеганосистем стійкість, як правило, оцінюють через кількість помилок, що виникли при вилучені повідомлення з контейнера легальним користувачем після можливих спотворень цього контейнера ненавмисними чи активними атаками. Наприклад, дослідження стійкості до процесів друку та сканування, що обов’язково супроводжують стеганоконтейнер у задачах захисту інформації на паперових носіях.

Необхідний рівень стійкості визначається застосуванням системи. Так, говорячи про стійкість до активних атак, виділяють системи ЦВЗ зі стійкими, крихкими та напівкрихкими водяними знаками [51]. Розглянемо детальніше стійкість у моделях пасивного та активного противників.

Стеганосистема та відповідно стеганоконтейнери, які вона продукує, вважаються стійкими до пасивних атак тоді і тільки тоді, коли несанкціонований користувач не має можливості відрізнити пусті контейнери від заповнених, зокрема методами візуального та статистичного аналізу.

Більша частина поширених програмних продуктів для прихованої передачі інформації методами комп’ютерної стеганографії, реалізують різні модифікації методу найменшого значущого біту, суть якого полягає у заміні молодших бітів контейнера бітами приховуваного повідомлення. Користувач обирає довільний контейнер, розміри якого дозволяють розмістити у ньому повідомлення, і в результаті отримує стеганоконтейнер, що візуально не відрізняється від пустого[45].

Між молодшими бітами сусідніх елементів природних контейнерів, а також між молодшим та іншими бітами елементів контейнера існує кореляційний зв'язок, що може бути порушеним вкрапленням повідомлення. У цьому випадку для виявлення стеганоконтейнера достатньо найпростішого аналізу – візуального аналізу бітових зрізів. Як правило, через наявність похибки квантування при оцифровці та інших шумів цифрові контейнери, що отримані з аналогових, більш

стійкі до такої атаки, ніж ті, що були створені відразу цифровими. Разом з тим, вкраплюючи повідомлення в НЗБ зашумленого контейнера, необхідно розподіляти його по всьому об’єму молодших бітів, інакше різниця між не зміненою та зміненою вкрапленням частинами може бути виявлена візуальною атакою на відповідний бітовий зріз.

Ємність. Ємність визначається як максимальна кількість даних повідомлення, які можуть бути вкрапленими в один елемент контейнера з дотриманням вимог невідчутності та стійкості.

На сьогоднішній день існують різні, іноді діаметрально протилежні підходи до визначення кількості приховуваної інформації. Ці розбіжності обумовлені відмінностями в цілях захисту інформації, видах порушника, їх можливостях, типах контейнерів та повідомлень та іншими факторами. Зокрема, в якості теоретично досяжних границь, що не залежать від особливостей практичного застосування, використовують оцінку пропускної здатності, отриману в теоретико-інформаційній моделі стеганосистеми [1].

Ємність визначає потенційний об’єм інформації, яку можна приховати тим чи іншим методом стеганографії. А той об’єм, що був реально використаний в процесі стеганоперетворення певного контейнера (тобто вкраплення в нього додаткової інформації), будемо називати наповненістю контейнера. Очевидно, що в рамках тієї чи іншої стеганосистеми наповненість будь-якого контейнера не може перевищувати пропускної здатності створюваного нею стеганоканалу. Наповненість зручно вимірювати у відсотках від пропускної здатності. Так, наповненість пустого контейнера складає 0%, максимально заповненого – 100%.

2.2 Галузі застосування

Цифрова стеганографія як наука народилася буквально в останні роки. Вона містить у собі такі напрями:

- вбудовування інформації з метою її прихованої передачі;
- вбудовування цифрових водяних знаків (ЦВДЗн) (watermarking);
- вбудовування ідентифікаційних номерів (fingerprinting);

– вбудовування заголовків (captioning).

ЦВДЗн можуть застосовуватися, в основному, для захисту від копіювання та несанкціонованого використання. У зв’язку з бурхливим розвитком технологій мультимедіа гостро встало питання захисту авторських прав і інтелектуальної власності, представленої в цифровому 9 вигляді. Прикладами можуть бути фотографії, аудіо- та відеозаписи та ін. Переваги, які дають подання та передача повідомлень у цифровому вигляді, можуть виявитися перекресленими з легкістю, з якою можливі їх викрадення або модифікація. Тому розробляються різні засоби захисту інформації, організаційного та технічного характеру. Один з найбільш ефективних технічних засобів захисту мультимедійної інформації полягає у вбудовуванні в захисті об’єкта невидимих міток – ЦВДЗн. Розробки в цій сфері ведуть найбільші фірми в усьому світі. Оскільки методи ЦВДЗн почали розроблятися зовсім недавно, то тут є багато неясних проблем, що вимагають свого вирішення[11].

Назву цей метод одержав від усім відомого способу захисту цінних паперів, у тому числі грошей, від підробки. Термін "digital watermarking" був уперше застосований у роботі [51]. На відміну від звичайних водяних знаків ЦВДЗн можуть бути не тільки видимими, але й, як правило, невидимими. Невидимі ЦВДЗн аналізуються спеціальним декодером, що виносить рішення про їх коректність. ЦВДЗн можуть містити деякий автентичний код, інформацію про власника або яку-небудь керуючу інформацію. Найбільш придатними об’єктами захисту за допомогою ЦВДЗн є нерухливі зображення, файли аудіо- й відеоданих[43].

Технологія вбудовування ідентифікаційних номерів виробників має багато загального з технологією ЦВДЗн. Відмінність полягає в тому, що в першому випадку кожна захищена копія має свій унікальний вбудований номер (звідси й назва – дослівно "відбитки пальців"). Цей ідентифікаційний номер дозволяє виробникові відслідковувати подальшу долю свого дітища: чи не зайнявся хто-небудь із покупців незаконним тиражуванням. Якщо так, то "відбитки пальців" швидко вкажуть на винного.

Вбудовування заголовків (невидиме) може застосовуватися, наприклад, для підпису медичних знімків, нанесення легенди на карту й т.д. Метою є зберігання різнорідно представленої інформації в єдиному цілому. Це, мабуть, єдиний додаток стеганографії, де в явному вигляді відсутній потенційний зловмисник.

Оскільки цифрова стеганографія є молодою наукою, то її термінологія не до кінця сформувалася. Основні поняття стеганографії були погоджені на Першій міжнародній конференції з приховання даних [21]. Проте навіть саме поняття "стеганографія" трактується по-різному. Так, деякі дослідники розуміють під стеганографією тільки приховану передачу інформації. Інші відносять до стеганографії такі додатки, як наприклад, метеорний радіозв'язок, радіозв'язок із псевдовипадковою перебудовою радіочастоти, широкосмуговий радіозв'язок. Неформальне визначення того, що таке цифрова стеганографія, могло б виглядати в такий спосіб: "наука про непомітне і надійне приховання одних бітових послідовностей в інших, що мають аналогову природу". Під це визначення саме підпадають всі чотири вищенаведені напрями приховання даних, а додатка радіозв'язку – немає. Крім того, у визначенні міститься дві головні вимоги до стеганографічному перетворення: непомітність і надійність, або стійкість до різного роду перекручування. Згадування про аналогову природу цифрових даних підкреслює той факт, що вбудовування інформації виконується в оцифровані безперервні сигнали. Таким чином, у рамках цифрової стеганографії не розглядаються питання впровадження даних у заголовки IP-пакетів і файлів різних форматів, у текстові повідомлення[40].

Яким б різними не були напрями стеганографії, пропоновані ними вимоги багато в чому збігаються, як це буде показано далі. Найбільш істотна відмінність постановки завдання прихованої передачі даних від постановки завдання вбудовування ЦВДЗн полягає в тому, що в першому випадку зловмисник повинен виявити приховане повідомлення, тоді як у другому випадку про його існування всі знають. Більше того, у зловмисника на законних підставах може бути пристрій виявлення ЦВДЗн (наприклад, у складі DVD-програвача).

Під словом "непомітний" у нашому визначенні цифрової стеганографії мається на увазі обов’язкове включення людини в систему стеганографічної передачі даних. Людина тут може розглядатися як додатковий приймач даних, що висуває до системи передачі досить важко формалізовані вимоги.

На рисунку 2.1 наведена класифікація систем цифрової стеганографії. Стеганосистема утворює стеганоканал, по якому передається заповнений контейнер. Цей канал уважається підданим впливам з боку порушників. Згідно з Г. Сіммонсом [63], у стеганографії звичайно розглядається така постановка завдання ("проблема ув’язнених").

Двоє ув’язнених, Аліса і Боб бажають конфіденційно обмінюватися повідомленнями, незважаючи на те, що канал зв’язку між ними контролює охоронець Віллі. Для того щоб таємний обмін повідомленнями був можливий, передбачається, що Аліса і Боб мають деякий відомий обом секретний ключ. Дії Віллі можуть полягати не тільки в спробі виявлення прихованого каналу зв’язку, але й у руйнуванні переданих повідомлень, а також їх модифікації та створенні нових, помилкових повідомлень. Відповідно можна виділити три типи порушників, яким повинна протистояти стеганосистема: пасивний, активний і злочинний порушники. Помітимо, що пасивний зловмисник може бути лише в стеганосистемах прихованої передачі даних. Для систем ЦВДЗ характерні активні та злочинні порушники[29].

Рисунок 2.1 – Класифікація систем цифрової стеганографії

Для того щоб стеганосистема була надійною, необхідне виконання при її проектуванні ряду вимог.

Безпека системи повинна повністю визначатися таємністю ключа. Це означає, що зловмисник може повністю знати всі алгоритми роботи стеганосистеми та статистичні характеристики множин повідомлень і контейнерів, і це не дасть йому ніякої додаткової інформації про наявність або відсутність повідомлення в даному контейнері.

Знання зловмисником факту наявності повідомлення в якому-небудь контейнері не повинне допомогти йому при виявленні повідомлень в інших контейнерах.

Заповнений контейнер повинен візуально не відрізнятися від незаповненого. Для задоволення цієї вимоги треба, здавалося б, впроваджувати приховане повідомлення у візуально незначущі множини сигналу. Однак ці ж множини

використовують і алгоритми стиску. Тому, якщо зображення буде надалі піддаватися стиску, то приховане повідомлення може зруйнуватися. Отже, біти повинні вбудовуватися у візуально значущі множини, а відносна непомітність може бути досягнута за рахунок використання спеціальних методів, наприклад, модуляції з розширенням спектра[20].

Стеганосистема ЦВДЗ повинна мати низьку ймовірність помилкового виявлення прихованого повідомлення в сигналі, що його не утримує. У деяких додатках таке виявлення може привести до серйозних наслідків. Наприклад, помилкове виявлення ЦВДЗ на DVD-диску може викликати відмову від його відтворення плеєром.

Повинна забезпечуватися необхідна пропускна здатність (ця вимога актуальна, в основному, для стеганосистем прихованої передачі інформації). У третьому розділі введемо поняття прихованої пропускної здатності й розглянемо шляхи її досягнення.

Стеганосистема повинна мати прийнятну обчислювальну складність реалізації. При цьому можлива асиметрична за складністю реалізації система ЦВДЗ, тобто складний стеганокодер і простий стегано-декодер.

До ЦВДЗ висуваються такі вимоги [5,11,55]:

- ЦВДЗ повинен легко (обчислювально) витягатися законним користувачем;
- ЦВДЗ повинен бути стійким або нестійким до навмисних і випадкових впливів.

Якщо ЦВДЗ використовується для підтвердження дійсності, то неприпустима зміна контейнера повинна призводити до руйнування ЦВДЗ (тендітний ЦВДЗ). Якщо ж ЦВДЗ містить ідентифікаційний код, логотип фірми тощо, то він повинен зберегатися при максимальних перекручуваннях контейнера, що звичайно, не приводять до істотних перекручувань вихідного сигналу. Наприклад, у зображенні можуть бути відредаговані колірна гама або яскравість, в аудіозаписі – посилене звучання низьких тонів і т.п. Крім того, ЦВДЗ повинен бути роботоздатним стосовно афінних перетворень зображення, тобто його поворотів, масштабування.

При цьому треба розрізняти стійкість самого ЦВДЗ і здатність декодера правильно його виявити. Скажемо, при повороті зображення ЦВДЗ не зруйнується, а декодер може виявитися нездатним виділити його. Існують додатки, коли ЦВДЗ повинен бути стійким стосовно одних перетворень і нестійким стосовно інших. Наприклад, може бути дозволене копіювання зображення (ксерокс, сканер), але накладена заборона на внесення в нього яких-небудь змін[27].

Повинна бути можливість додавання до стега додаткового ЦВДЗ. Наприклад, на DVD-диску є мітка про допустимість однократного копіювання. Після здійснення такого копіювання необхідно додати мітку про заборону подальшого копіювання. Можна було б, звичайно, видалити перший ЦВДЗ і записати на його місце другий, однак це суперечить припущенню про важковіддаленністю ЦВДЗ. Кращим виходом є додавання ще одного ЦВДЗ, після якого перший не буде братися до уваги. Однак наявність декількох ЦВДЗ на одному повідомленні може полегшити атаку з боку зловмисника, якщо не почати спеціальних заходів.

У цей час технологія ЦВДЗ перебуває в початковій стадії свого розвитку. Як показує практика, повинно пройти років 10 – 20 для того, щоб новий криптографічний метод почав широко використовуватися в суспільстві. Напевно, аналогічна ситуація буде спостерігатися й зі стеганографією. Однією із проблем, пов’язаних зі ЦВДЗ, є різноманіття вимог до них, залежно від додатка. Розглянемо докладніше основні множини застосування ЦВДЗ.

Спочатку розглянемо проблему піратства, або необмеженого неавторизованого копіювання. Наприклад, Аліса продає своє мультимедійне повідомлення Пітеру. Хоча інформація могла бути зашифрована під час передачі, ніщо не перешкодить Пітеру зайнятися її копіюванням після розшифровки. Отже, у цьому випадку потрібен додатковий рівень захисту від копіювання, що не може бути забезпечений традиційними методами. Існує можливість впровадження ЦВДЗ, що дозволяє відтворення та забороняє копіювання інформації[30].

Важливою проблемою є визначення дійсності отриманої інформації, тобто її автентифікація. Звичайно для автентифікації даних використовуються засоби цифрового підпису. Однак ці засоби не зовсім підходять для забезпечення

автентифікації мультимедійної інформації. Справа в тому, що повідомлення, постачене електронним цифровим підписом, повинне зберігатися й передаватися абсолютно точно, "бітів у бітів". Мультимедійна ж інформація може незначно спотворюватися як при зберіганні (за рахунок стиску), так і при передачі (вплив одиночних або пакетних помилок у каналі зв’язку). При цьому її якість залишається припустимою для користувача, але цифрової підпис працювати не буде. Одержувач не зможе відрізнити справжнє, хоча і трохи перекручене повідомлення, від помилкового. Крім того, мультимедійні дані можуть бути перетворені з одного формату в інший. При цьому традиційні засоби захисту цілісності працювати також не будуть[69].

Можна сказати, що ЦВДЗ здатно захистити саме зміст аудіо-, відеоповідомлення, а не його цифрове подання у вигляді послідовності бітів. Крім того, важливим недоліком цифрового підпису є те, що його легко видалити із завіреного ним повідомлення, після чого прилаштувати до нього новий підпис. Видалення підпису дозволить зловмиснику відмовитися від авторства, або ввести в оману законного одержувача щодо авторства повідомлення. Система ЦВДЗ проектується таким чином, щоб виключити можливість подібних порушень. Як видно з рис. 1.3 застосування ЦВДЗ не обмежується додатками безпеки інформації.

Рисунок 2.2 – Потенційні множини застосування стеганографії

Основні множини використання технології ЦВДЗ можуть бути об’єднані в чотири групи: захист від копіювання (використання), прихована анотація документів, доказ автентичності інформації та прихований зв’язок.

Популярність мультимедіа-технологій викликало множину досліджень, пов’язаних з розробкою алгоритмів ЦВДЗ для використання в стандартах MP3, MPEG-4, JPEG2000, захисту DVD-дисків від копіювання

2.3 Стеганографічні середовища

Революція в комп'ютерних технологіях та Інтернеті дала стеганографії особливу важливість. Багато змін трапилося з вітчизняними носіями завдяки застосуванню стеганографії в комп'ютерних технологіях. Ці носії можуть бути віднесені до багатьох видів даних, таких як текст, диск, аудіо, зображення, звук, мережевий трафік або інші дані цифрової передачі даних. Способи приховування даних наведено нижче[28].

Приховування в тексті. Для приховування інформації у тексті (лінгвістична стеганографія) використовується звичайна надлишковість письмової мови або формати представлення тексту.

Найскладнішим об’єктом для приховування є електронна версія тексту, тому що його друкована версія може бути зображенням в електронному вигляді, обробленим відповідними методами. Ця складність в основному обумовлена відносним дефіцитом у тексті надлишковості, на відміну від зображення або аудіо-файлу. В той час як існує можливість внести невидимі для ока модифікації у зображення або не відчутні для слухової системи людини (ССЛ) зміни у звучанні аудіофайла, будь-яка зайва літера, зайвий символ або зайвий знак пунктуації може бути виявлений випадковим читачем[39].

Існують три основні методи приховування даних у тексті, що найширше розповсюджені:

- методи довільних інтервалів;
- синтаксичні методи;
- семантичні методи.

Приховування в зображеннях. В більшості випадків використовуються стеганографічні методи із графічними зображеннями в ролі контейнерів саме через такі причини:

- розповсюдження цифрових фотографій та відео, які необхідно захищати від протизаконного тиражування та розповсюдження;
- відносно великий об’єм графічних зображень, що дає широкий простір для приховування даних (великого розміру);
- розмір контейнера відомий заздалегідь, що дає змогу обирати оптимальний контейнер;
- відносно слабка чутливість людського ока до незначних змін у цифрових графічних зображеннях;
- добре розроблені, в останній час, методи цифрової обробки зображень.

Приховування у відео файлах. Стеганографічні методи приховування рідше за все використовуються у відеоданих, оскільки даний файл складається з динамічних зображень (фреймів) та звукової доріжки. Варто також зазначити, що досі не використовуються як контейнери одночасно аудіодоріжки та фрейми.

На сьогодні існує три методи для приховування інформації у відеоданих, а саме:

Метод вбудовування на рівні коефіцієнтів – біти приховуваного повідомлення вбудовуються в коефіцієнти ДКП. Враховуючи, що використовуються алгоритми стиснення, основною проблемою стає накопичення зсуву та помилок. Для зменшення внесених змін використовують додатковий спеціальний сигнал. В зв'язку з обмеженням бітової швидкості при вбудовуванні змінюється лише 10-12% коефіцієнтів ДКП. При використанні даного методу приховувана інформація зберігається при фільтруванні, зашумленні (адитивним шумом) і дискретизації[56].

Метод вбудовування інформації на рівні бітової площини - відрізняється високою пропускною здатністю і легкими обчисленнями. Але є й істотний недолік: інформація, вбудована таким чином, може бути легко видалена. При повторному накладенні послідовності біт якість відео погіршиться, а приховувана інформація буде знищена.

Метод вбудовування інформації за рахунок енергетичної різниці між коефіцієнтами - в основі лежить диференціальне вбудовування енергії. Цей метод може використовуватись для багатьох алгоритмів стиснення. Інформація вбудовується шляхом видалення декількох коефіцієнтів ДКП [65].

В основному, приховування в відео використовує методи, які використовуються для приховування звуку та зображення, оскільки вже є відеозображеннями зображень і звуків. Відео складається з переміщення зображень в супроводі з аудіо. Ннасправді це є перевагою, оскільки будь-які невеликі спотворення користувачі навіть не помітять через неперервну кількість даних.

Приховування в аудіо файлах. Особливий розвиток отримали стеганографічні методи приховування інформації у аудіосередовищі. Це охарактеризовано тим, що ССЛ працює у надширокому динамічному діапазоні і має

доволі малий різницевий діапазон. Виходячи із цього, можна зробити висновок, що у аудіофайлах присутній широкий простір для приховування даних. Також ССЛ не здатна розрізняти абсолютну фазу, вирізняє лише відносну. Крім того, існують деякі види спотворень, викликаних зовнішнім середовищем, які можна використати для приховування даних[28].

Приховування даних в аудіо файлах особливо складне через його великий діапазон частот. Аудіосигнали також чутливі до випадкових шумів. Шум може бути виявлений, якщо він знаходиться в діапазоні від одного до мільйону у звукових файлах.

При приховуванні звуку користувач повинен скористатися перевагами слабкості людського слухового апарату, але також слід подбати про його високу чутливість.

2.4 Методи стеганографії аудіо файлів

Існує декілька способів приховування інформації або повідомлень у аудіо таким чином що зміни, внесені до аудіофайлу, є перцептивно нерозбірливими. Загальні підходи включають [2, 3]:

2.4.1 LSB кодування

Дуже популярною методологією є LSB (найменший значущий біт) алгоритм, який замінює найменш значущий біт в деяких байтах файлу обкладинки, щоб приховати послідовність байтів, що містять приховані дані. Це, як правило, ефективна методика у випадках, коли заміни LSB не викликають значне погіршення якості.

У обчисленні, найменш значний біт (LSB) - це бітна позиція у двійковому цільовому числу, що дає одичні значення, тобто визначає чи є число парним або непарним. Іноді згадується LSB як найправильніший біт, завдяки конвенції в позиційному позначенні писати менш значущі цифри далі вправо. Він аналогічний найменш значущому знаку десяткового цілого числа, тобто цифра у крайній (праворуч) позиції.

Бінарне представлення десяткового числа 149 з підсвічуванням LSB. MSB у 8-бітовому двійковому значенні представляє значення 128 десяткових знаків. LSB

представляє значення 1. Наприклад, щоб приховати букву "a" (ASCII-код 97, тобто 01100001) всередині восьми байт кришки, ви можете встановити LSB кожного байта таким чином:

10010010
01010011
10011011
11010010
10001010
00000010
01110010
00101011

Програма, яка декодує кришку, зчитує вісім найменших значущих бітів з цих байтів, щоб відтворити прихований байт - це 0110001 - буква "a". Як ви можете зрозуміти, використовуючи цей метод, ви можете приховати байт кожні вісім байт обкладинки. Зверніть увагу, що існує п'ятдесят відсотків шансів, що біт, який ви замінюєте, той самий, що і його заміна, тобто половину часу, біт не змінюється, що допомагає мінімізувати якісну деградацію.

Цей метод є одним з найпопулярніших, що вивчаються при приховуванні інформації цифрового звуку (а також інших типів носіїв). У цій техніці LSB, послідовності кожного зразка оцифрованого аудіофайлу замінюється на двійковий еквівалент секретного повідомлення. Це найпростіший спосіб вставляти інформацію в цифровий аудіо файл. Це дозволяє приховати велику кількість даних у аудіофайлі або забезпечити високу швидкість вкладання без погіршення якості звукового файла [19]. Використання тільки одного LSB зразка аудіо-хосту дає потужність, еквівалентну частоті дискретизації, яка може варіюватися від 8 кбіт / с до 44,1 кбіт / с [20].

У LSB кодування ідеальна швидкість передачі даних становить 1 кбіт / с на 1 кГц. Однак у деяких варіантах кодування LSB, два найменш значущих біти замінюються двома бітами повідомлення. Це збільшує кількість даних, які можна

кодувати, але також збільшує кількість шуму, що виникає, у аудіофайлі. Таким чином, слід враховувати вміст сигналу, перш ніж приймати рішення про використання операції LSB.

Наприклад, звуковий файл, який був записаний на шумній станції метро, маскує низькошвидкісний шум кодування. З іншого боку, той же звук буде звучати в звуковому файлі, що містить фортепіано соло. Щоб витягти секретне повідомлення з звукового файлу, закодованого LSB, одержувач потребує доступу до послідовності індексів вибірки, які використовуються в процесі вбудовування. Як правило, довжина секретного повідомлення, що підлягає кодуванню, менша, ніж зразки звукового файла. Потім треба вирішити, як вибрати 7 підмножин зразків, які містять секретне повідомлення, і повідомити про це рішення одержувачу. Одна тривіальна методика полягає в тому, щоб почати з початку звукового файла та виконувати кодування LSB, поки повідомлення не буде повністю вбудовано; залишаючи залишкові зразки незмінними. Це створює проблему безпеки, однак в тому, що перша частина звукового файлу матиме різні статистичні властивості, ніж друга частина не зміненого звукового файлу [21]. Одне рішення цієї проблеми полягає в тому, щоб поставити секретне повідомлення з випадковими бітами, так щоб довжина повідомлення дорівнювала загальній кількості зразків. Проте зараз процес введення закінчується зміною набагато більшої кількості зразків, ніж передача потрібного секрету. Це збільшує ймовірність того, що майбутній зловмисник викриє секретне спілкування. Після виконання програми процедура може бути показана за допомогою оригінальних даних, як показано на рисунку 2.3:

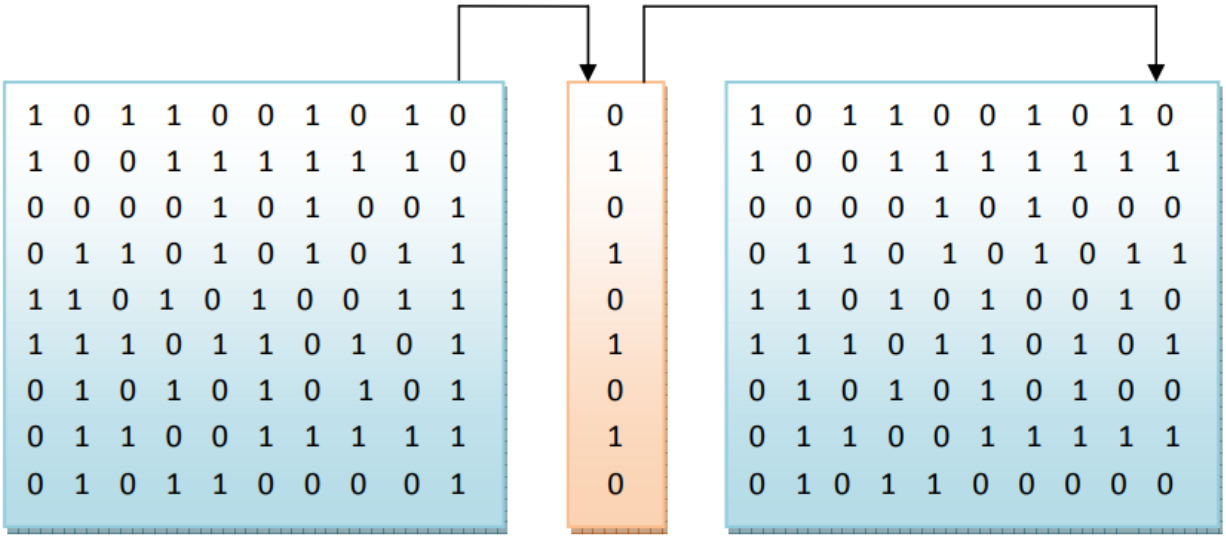

Рисунок 2.3 – Метод LSB для аудіо стеганографії

Більш витончений підхід полягає у використанні генератора псевдовипадкових чисел, щоб розповсюджувати повідомлення над звуковим файлом у випадковому порядку. Одним із популярних підходів є використання методу випадкових інтервалів, в якому секретний ключ, яким володіє відправник, використовується як насіння в генераторі псевдовипадкових чисел для створення випадкової послідовності індексів вибірки. Приймач також має доступ до секретного ключа та знань генератора псевдовипадкових чисел, що дозволяє відновлювати випадкову послідовність показників вибірки.

Однак перевірки повинні бути встановлені, щоб запобігти генерації псевдовипадкового числа двічі. Якщо це сталося, виникне зіткнення, коли зразок, уже змінений частиною повідомлення, буде змінено знову. Проблему зіткнень можна подолати, відстежувати всі вже використані зразки. Інший підхід полягає у розрахунку підмножини зразків за допомогою псевдовипадкової перестановки всього набору за допомогою безпечної хеш-функції. Ця методика гарантує, що один і той же індекс ніколи не генерується більше одного разу[56].

2.4.2 Паритетне кодування

Паритетне кодування - це один з надійних звукових стеганографічних методів. Замість того, щоб розбити сигнал на окремі зразки, цей метод розбиває сигнал на окремі зразки і вставляє кожен біт секретного повідомлення в біт парності. Якщо біт

парності обраної області не збігається з секретним бітом, який буде кодуватися, процес інвертує LSB одного з зразків у регіоні. Отже, відправник має більше вибору при кодуванні секретного біта[33].

Використовуючи метод паритетного кодування, перші три біти повідомлення "HEY" закодовані на наступному рисунку 2.4.

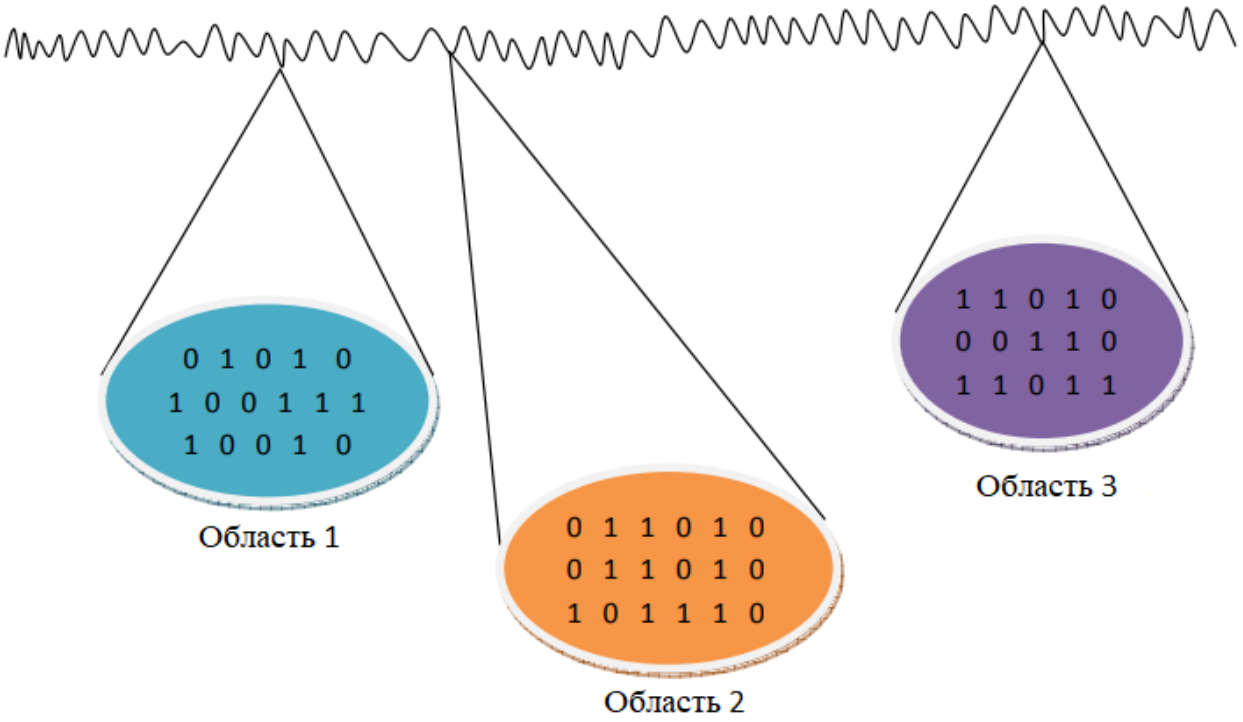

Рисунок 2.4 – Метод паритетного кодування

Процес декодування витягує таємне повідомлення, обчислюючи і виділяючи біти парності регіонів, що використовуються в процесі кодування. Знову ж таки, відправник і одержувач можуть використовувати загальний секретний ключ як насіння у генераторі псевдовипадкових чисел, щоб створити той самий набір зразків областей. Існує два основних недоліки, пов'язані з використанням таких методів, як кодування LSB або кодування рівності. Людське вухо дуже чутливе і може часто виявляти навіть найменший шум, введений у звуковий файл, хоча метод паритетного кодування досить наближений до того, щоб введений шум був не чутним.

Обидва способи мають ще один недолік, оскільки вони не є надійними. Якщо звуковий файл, вбудований в секретне повідомлення з кодуванням LSB або кодування рівності, був повторним зразком, вбудована інформація буде

втрачена[66]. Потужність може дещо покращити, використовуючи техніку резервування при кодуванні секретного повідомлення. Однак технології резервування значно зменшують швидкість передачі даних.

2.4.3 Фазове кодування

Технологія фазового кодування працює шляхом заміни фази початкового аудіо сегменту з еталонною фазою, що представляє секретну інформацію. Решта фази сегментів коригується для збереження відносної фази між сегментами. З точки зору співвідношення сигнал / шум, фазове кодування є одним з найбільш ефективних методів кодування. Коли відбувається різка зміна фазового зв'язку між кожною частотною складовою, спостерігається помітна дисперсія фази. Однак до тих пір, поки модифікація фази буде достатньо мала, може бути досягнуте неголосне кодування [35]. Цей метод спирається на те, що фазові компоненти звуку не так сприймаються людському вухо, як це звучить.

Фазове кодування розглядає недоліки шумопоглинаючих методів аудіо стеганографії. Фазове кодування залежить від того, що фазові компоненти звуку не настільки чутливі для людського вуха, як шум. Замість того, щоб вводити збурення, ця техніка кодує біти повідомлень у вигляді фазових зрушень у фазовому спектрі цифрового сигналу, досягаючи безшумного кодування у співвідношенні сигнал/шум. Або можна сказати, що фазове кодування залежить від заміни вибраних фазових компонентів прихованими даними. Відзначено, що серед усіх методів приховування, фазове кодування перешкоджає кращому перекручуванню сигналу. Фазове кодування вставляє дані в фазові компоненти, використовуючи незалежну багатодіапазонну фазову модуляцію. У такому підході непомітна фазова модифікація досягається за допомогою керованої фазової зміни аудіо-хоста, показаного на рисунку 2.5. Оригінальний звуковий сигнал розбитий на менші сегменти, довжини яких дорівнюють розміру кодуваного повідомлення.

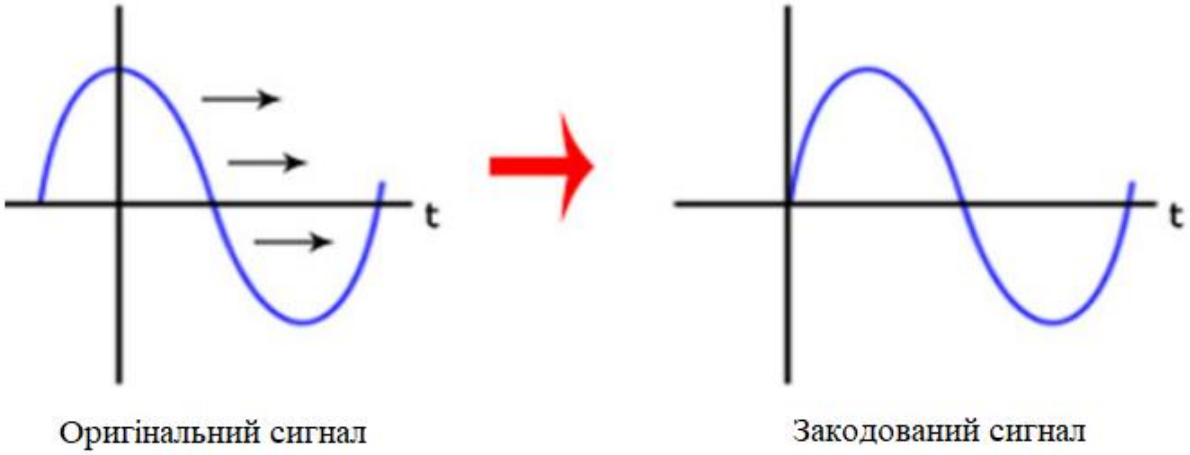

Рисунок 2.5 – Метод фазового кодування

Фазове кодування пояснюється в наступному порядку:

– Розділіть оригінальний звуковий сигнал на менші сегменти, такі, щоб довжини були такого ж розміру, як і розмір кодуваного повідомлення.
– Матриця фаз створюється шляхом застосування дискретного перетворення Фур'є (DFT).
– Обчислити відмінності фаз між суміжними сегментами.
– Фазові зрушення між суміжними сегментами легко виявляються. Це означає, що ми можемо змінити абсолютні фази сегментів, але відносні відмінності фаз між суміжними сегментами повинні бути збережені. Таким чином, секретна інформація вставляється тільки в вектор фази першого сегмента сигналу наступним чином:

$$\text{фаза} = \begin{cases} \frac{\pi}{2}, \text{якщо біт} = 0 \\ -\frac{\pi}{2}, \text{якщо біт} = 1 \end{cases}$$

– Використовуючи нову фазу першого сегмента, створюється нова фазова матриця та вихідні відмінності фаз.
– Звуковий сигнал реконструюється шляхом застосування зворотного дискретного перетворення Фур'є з використанням нової фази матриці та матриці оригінальної величини, а потім об'єднує сегменти звуку назад

Приймач повинен знати довжину сегмента для вилучення секретної інформації з звукового файлу. Тоді приймач може використовувати ДПФ, щоб отримати етапи та витягнути секретну.

Одним з недоліків, пов'язаних з фазовим кодуванням, є низька швидкість передачі даних через те, що таємне повідомлення кодується лише в першому сегменті сигналу. Це може бути вирішено шляхом збільшення довжини сегмента сигналу[47].

Однак це змінить фазові зв'язки між кожною частотною складовою сегмента більш різко, що робить кодування легшим для виявлення. Як наслідок, метод фазового кодування використовується, коли потрібно приховати лише невелику кількість даних, таких як водяний знак.

2.4.4 Розповсюдження спектру

У аудіо стеганографії основний метод розповсюдження спектру намагається поширювати секретну інформацію по частотному спектру аудіосигналу. Це схоже на систему, яка використовує реалізацію LSB, яка поширює біти повідомлень випадковим чином по всьому звуковому файлу. Проте, на відміну від кодування LSB, метод розповсюдження спектру поширює секретну інформацію по частотному спектру звукового файлу за допомогою коду, який не залежить від фактичного сигналу [20]. Як результат, кінцевий сигнал займає смугу пропускання, яка перевищує те, що дійсно потрібно для передачі.

Метод розповсюдження спектру здатний сприяти поліпшенню продуктивності в деяких областях порівняно з кодуванням LSB та фазовим кодуванням, оскільки він забезпечує помірну швидкість передачі даних і високий рівень надійності відносно методів видалення. Проте метод розповсюдження спектру має один основний недолік, який може вводити шум у звуковий файл.

2.4.5 Приховування відлуння

Техніка приховування відлуння використовує секретну інформацію у звуковому файлі, вводячи відлуння в дискретний сигнал. Приховування відлуння має переваги забезпечення високої швидкості передачі даних і вищої надійності в

порівнянні з іншими методами. Лише один біт секретної інформації може бути закодований, якщо тільки вихідний сигнал було отримав лише одне відлуння.

Отже, перед початком процесу кодування оригінальний сигнал розбитий на блоки. Після завершення процесу кодування блоки об'єднуються разом, щоб створити остаточний сигнал[66].

Для успішного приховання даних, три параметри відлуння повинні бути різними: амплітуда, швидкість розпаду та зміщення (час затримки) від вихідного сигналу. Всі три параметри встановлені нижче порогу слуху людини, тому відлуння не може бути легко виявлено. Крім того, зміщення змінюється, щоб представляти бінарне повідомлення для кодування. Одне значення зміщення являє собою двійкове значення, а значення другого зміщення являє собою двійковий нуль. Зміщення представлено на рисунку 2.6.

Рисунок 2.6 – Значення відступів відтворюють двійкові значення

Якщо вихідний сигнал був вироблений лише одним відлуння, кодування може містити лише один біт інформації. Тому початковий сигнал розбивається на блоки, перш ніж процес кодування починається. Після завершення процесу кодування, блоки об'єднуються разом, щоб створити остаточний сигнал[50]. Тепер ми пройдемо просту форму процесу приховування відлуння, використовуючи повідомлення "HEY". Для стислості сигнал буде повністю розділений на блоки, хоча за звичайних

умов випадкова кількість зразків між кожною парою блоків повинна залишатись невикористаною, щоб зменшити ймовірність виявлення. Перестановка остаточних блоків представлена на рисунку 2.7.

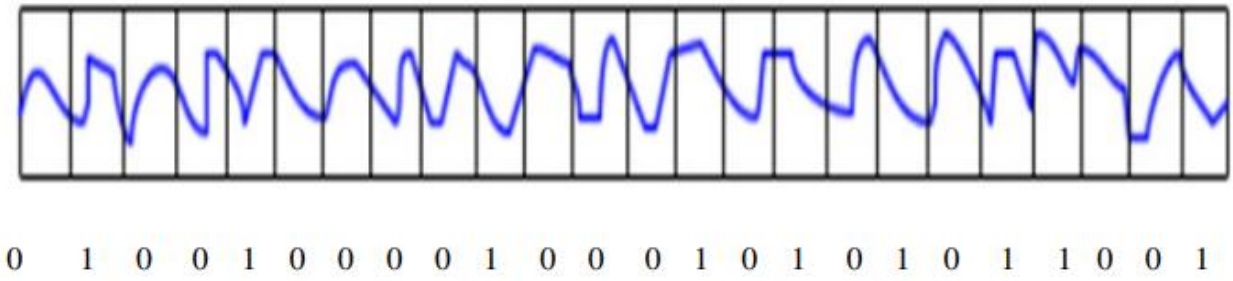

Рисунок 2.7 – Блоки переставляються для отримання остаточного сигналу

Спочатку сигнал ділиться на блоки, і кожному блоку присвоюється один чи нуль, що базується на секретному повідомленні. У цьому випадку повідомлення є двійковим еквівалентом "HEY".

Використовуючи цю реалізацію процесу приховування відлуння, зазвичай може бути отриманий сигнал, який має досить помітний набір відлуння, що підвищує ризик виявлення. Друга реалізація процесу приховування відлуння вирішує цю проблему. Спочатку відлуння створюється з усього вихідного сигналу, використовуючи значення двосмугового зсуву нуля. Потім другий сигнал відлуння створюється з усього вихідного сигналу, використовуючи значення двосмугового зсуву. Таким чином, "один" відлуння містить тільки одиниці, а "нульовий" відлуння містить тільки нулі. Щоб об'єднати два відлуння разом, щоб отримати остаточне кодування, використовуються два сигнали змішувача.

Сигнали змішувача мають значення як одиниці, так і нулі, в залежності від того, який біт потрібно кодувати в блоці. "Один" сигналу відлуння помножується на "один" сигнал змішувача, а "нульовий" сигнал відлуння помножується на "нульовий" сигнал змішувача. Потім два результати додаються разом, щоб отримати остаточний сигнал. Остаточний сигнал є менш різким, ніж той, який був отриманий за допомогою першої реалізації приховування відлуння. Це пояснюється тим, що два ефекти змішувача є доповненнями один до одного, і ці переходи використовуються в кожному сигналі. Ці дві характеристики сигналів змішувача забезпечують більш плавні переходи між відлуннями. Щоб витягти таємне

повідомлення зі стемо-сигналу, приймач повинен мати можливість розбити сигнал на той же блоковий порядок, який використовується під час процесу кодування.

2.4.6 Порівняння методів

Обговоримо недоліки попередньої процедури та те, як вони відрізняються від поточного методу. Основні недоліки, пов'язані з використанням існуючих методів, таких як приховування відлуння, розповсюдження спектру та паритетне кодування, є дуже чутливим до шуму, і вони часто можуть виявляти навіть найменший шум, введений у звуковий файл, і інша проблема - це надійність.

Фазове кодування має основний недолік низької швидкості передачі даних через те, що секретне повідомлення кодується тільки в першому сегменті сигналу. Отже, цей метод використовується лише тоді, коли потрібно передати невелику кількість даних.

Серед різних методів приховування інформації, запропонованих для вбудовування секретної інформації в аудіофайл, найменш значущий біт (LSB) є найпростішим способом вбудовування секретної інформації в цифровий аудіо файл, замінивши найменш значущий біт аудіофайла з двійкового повідомлення. Тому метод LSB дозволяє кодувати велику кількість секретної інформації у аудіофайлі.

Порядок приховування секретної інформації за допомогою LSB:

- Приховати аудіо файл у бітовий потік.
- Перетворення кожного символу секретної інформації в бітовий потік.
- Заміна біту звуку LSB на біт символу LSB у секретній інформації.

Висновки до розділу

У межах розділу розкрито теоретичну сторону існуючих алгоритмів розв’язання задачі аудіо стеганографії. Проведено порівняння та розглянуто переваги та недоліки описаних методів.

Метод LSB забезпечує більшу безпеку та є ефективним способом приховування секретної інформації від хакерів і відправлення в пункт призначення безпечним та невиявленим способом. Ця запропонована система також гарантує, що розмір файлу не змінюється навіть після кодування, і також підходить для будь-якого типу формату аудіофайлів. Також він дозволяє приховувати в файлах

контейнерах набагото більший об'єм секретної інформації в порівнянні з іншими алгоритмами. Через його переваги над іншими алгормами, він був обраний для розроблення модифікації, яка описана в наступному розділі.

3. Модифікація алгоритму

3.1 Змістовна постановка задачі

Наразі, існують не мало методів стеганографії аудіо файлів. Основні недоліки використання таких методів як відлуння, розширеного спектру і паритетного кодування полягають в тому, що вони вносять шум в аудіо файл, який може бути досить помітним для людського вуха, а також надійність даних методів викликає питання. Щодо фазового кодування, то цей метод має основний недолік, що полягає в низькій швидкості передачі даних через те, що секретне повідомлення кодується тільки на першому сегменті сигналу. Отже, цей метод використовується тільки тоді, коли передається невелика кількість даних.

Серед вище запропонованих методів стеганографії метод найменшого значущого біта або LSB є найпростішим методом для вбудовування секретної інформації. Метод LSB дозволяє закодувати велику кількість даних в звуковий файл, забезпечує більш високий рівень безпеки в порівнянні з іншими методами, є ефективним методом для приховування секретної інформації від зловмисників, а також гарантує незмінність розміру файлу навіть після кодування і підходить для будь-якого типу формату аудіо файлу. Також він дозволяє приховувати в файлах контейнерах набагото більший об'єм секретної інформації в порівнянні з іншими алгоритмами.

Таким чином, проблема полягає в помітному спотворенні вхідного контейнеру та відсутності стійкості до атак.

3.2 Математична постановка задачі

Процес приховування повідомлення може бути представлений наступним чином:

$$\mathrm{E}\colon \mathrm{C} \times \mathrm{M} \to \mathrm{S},$$

де $S = \{ (c_1, m_1),\ (c_2, m_2), \dots ,\ (c_q, m_q),\} = \{s_1, s_2, \dots, s_q\}$ множина заповнених контейнерів (стегано-контейнерів), E – відображення, C – представляє всі можливі файли, в які будуть приховані секретні дані, а M - всі можливі секретні повідомлення.

Для вилучення будь-якого таємного повідомлення з файлу, який його містить, використовується наступне:

$$\mathrm{D}: \mathrm{M} \times \mathrm{C} \rightarrow \mathrm{M}$$

З необхідною умовою – відсутність перетину, тобто якщо:

$$m_a \neq m_b$$

при чому

$$m_a, m_b \in M \text{ та } (c_a, m_a),\ (c_b, m_b) \in S$$

то

$$E(c_a, m_a) \cap E(c_b, m_b) = \emptyset$$

В загальному випадку стеганосистему можна представити як сукупність ∑(C, M, S, E, D) – контейнерів, повідомлень та перетворень, що їх зв'язують. Завжди контейнери C обираються таким чином, щоб заповнений контейнер майже не відрізнявся від порожнього контейнера.

Стеганосистема може вважатися надійною, коли:

$$sim[c, E(c, m)] = 1$$

де sim – функція подібності.

Контейнер може обиратися двома способами: довільно (сурогатний метод) та підбором найбільш придатного у конкретному випадку контейнера, який зміниться найменше при перетворенні. В останньому випадку контейнер обирається виходячи із умови:

$$c = \max sim[c, E(c, m)]$$

В будь-якому випадку пряме та зворотне перетворення (E та D) мають відповідати одне одному та підлягати умові, що незначне викривлення контейнера (на величину δ) не має призводити до викривлення прихованої інформації:

$$E(c, m) \approx E(c + \delta, m)$$

або

$$D[E(c, m)] \approx D[E(c + \delta, m)] = m$$

3.3 Доступні набори даних

Як файли контейнери, так і секретні повідомлення в цій роботі є MP3-файли, оскільки вони забезпечують гарне стиснення даних. І враховуючи обмеження людськомго слуху, стиснення даних не впливає на сприйняття якості звуку. Більшість дослідників використовуюьт файли формуту wav, що призводить до наявності стандартного набору даних для нього. В нашому випадку, при використанні MP3 файлів обрано власний набір всіх вхідних даних. У цьому наборі даних міститься 10 різних жанрів: Класична, Джаз, Кантрі, R&B, Реп, Реггі, Поп, Рок, Блюз, Хіп-хоп.

Генерування MP3 файлів залежить від використання певної програми для перетворення кожного жанру з WAV-файлу в MP3-файл. З іншого боку, існує п'ять різних методів стиснення бітрейтів файлів MP3; 320 Кбіт/с, 256 Кбіт/с, 196 Кбіт/с, 128 Кбіт/с і 96 Кбіт/с. Їх значення відрізняються впливом на якість звуку. Іншими словами, збільшення кількості бітів на зразок призводить до підвищення якості звуку.

Наступна таблиця ілюструє стандартний набір даних MP3, який створений для використання в цій роботі.

Таблиця 3.1 – Набір вхідних даних (використовуються як секретне повідомлення)

Наймену-вання жанру	**Час, сек.**	**Розмір файлу (WAV), MB**	**Розмір файлу (320 кбіт/сек), MB**	**Розмір файлу (256 кбіт/сек), MB**	**Розмір файлу (192 кбіт/сек), MB**	**Розмір файлу (128 кбіт/сек), MB**	**Розмір файлу (96 кбіт/сек), MB**
Класична	2:42	14.4	6.54	5.24	3.94	2.62	1.97
Джаз	2:56	15.4	7.01	5.60	4.21	2.81	2.11
Кантрі	3:11	16.5	7.51	6.00	4.51	3.01	2.26
R&B	3:15	16.9	7.68	6.15	4.62	3.08	2.32
Реп	3:24	17.4	7.90	6.33	4.76	3.17	2.38
Реггі	3:42	18.2	8.27	6.62	4.98	3.32	2.49
Поп	3:53	19.1	8.68	6.95	5.22	3.48	2.62
Рок	4:04	20.3	9.22	7.38	5.55	3.70	2.78

Блюз	4:12	21.1	9.59	7.67	5.77	3.85	2.89
Хіп-хоп	4:27	22.7	10.31	8.25	6.21	4.14	3.11

В цьому дослідженні, вхідними даними, в якості файлів контейнерів виступають аудіо MP3 файли, по 20 файлів кожного із вище згаданих стилів музики.

3.4 Цілісність файлів після атаки

Значення хеш-функції. Це типовий метод перевірки цілісності даних, який широко використовується в різних протоколах та додатках. Він має суттєву роль у поточній криптографії. Основна ідея щодо хеш-функцій полягає в тому, що хеші виступають як компактний делегат, який називається відбитками чи цифровими відбитками вхідного об’єкту. Ці функції широко використовуються у перевірці цілісності даних у поєднанні з моделями цифрового підпису, оскільки повідомлення, як правило, спочатку хешуються, а потім замість оригінального повідомлення підписуються хеші.

Одним з основних класів хеш-функцій є коди аутентифікації повідомлень. Це дозволяє розпізнавати повідомлення за допомогою симетричних методів. Ця техніка приймає два основні вхідні параметри – повідомлення та секретний ключ. Основною метою є спрощення у поєднанні з подальшими механізмами цілісності даних для різних додатків. Функції без хешування можна розділити на два класи – односторонні хеш-функції, де знайти значення вхідних даних, для відомого хешу не є легкою задачею і стійкі до конфліктів хеш-функції, де пошук двох значень вхідних даних з одним і тим же значенням хешу не є легкою задачею.

Інший тип хеш-функцій - це виправлення модифікації, який пропонує 16 хеш-байтове значення. Ця функція широко використовується в криптографічних додатках та перевірці цілісності даних.

Контрольна сума. Контрольна сума є одним з основних методів перевірки цілісності. Її значення залежить від порівняння вхідного об'єкту зі значеннями отриманима після кодування. Цей метод в основному застосовується разом з розрахунком значень хеш-функцій.

Метод порівняння значень контрольної суми двох об'єктів допомагає виявити зміни цілісності. Однак він не може відновлювати дані через невідповідність між

вхідними та вихідними значеннями контрольних сум. Збережені контрольні суми можуть бути пошкоджені або змінені. Ще однією причиною проблеми відновлення значення контрольної суми є те, що вона обчислюється за допомогою односторонньої хеш-функції, коли дані не можна відновити, щоб отримати значення контрольної суми.

Контрольна сума використовується, щоб зменшити дублікати в об'єктах даних, оскільки ці дубльовані об'єкти мають однакове значення контрольної суми. Ці об'єкти можна розпізнати на основі використання раціональної колізійної моделі контрольної суми, тобто на основі порівняння значень контрольних сум цих об'єктів. Ще одне використання для контрольних сум можна знайти в індексування даних. Контрольна сума може також використовуватися для забезпечування простого способу отримання відповідних значень контрольних сум, що, у свою чергу, допомагає підвищити ефективність перевірки цілісності.

3.5 Опис модифікації методу

Розроблено модифікацію існуючого методу аудіо стеганографії найменш значущого біту (LSB). Було вирішено модифікувати саме цей метод, оскільки він надає змогу краплення набагато більших об’ємів повідомлень в порівнянні з іншими методами, але при цбому, сам метод можна вдосконалити з ціллю змншити помітних змін файлів контейнерів. Розроблена модифікація полягає в чередуванні місця заміни незначущого біту серед наймен значущих кожного зразка в файлі контейнері бітом секретного повідомлення для підвищення безпеки.

В процесі дослідження повинні бути виконані основні етапи: підготовка контейнеру та секретного повідомлення, вкраплення секретоного повідомлення, оцінка спотворення вхідного файлу, перевірка цілісності контейнерів, застосування атаки. Підготовка контейнеру та секретного повідомлення полягає у перевірці можливості вкраплення секретного повідомлення до контейнеру та перетворенні у двійковий формат даних. На етапі вкраплення секретоного повідомлення здійснюється саме приховування екретного повідомлення до файлу контейнеру нступними методами: традиційні 4-LSB, 2-LSB, 1-LSB та розроблена модифікація. Оцінка спотворення вхідного файлу перевіряється за допомогою розрахунку

коефіцієнту пікового сигналу до шумового співвідношення для кожного з стегано-контейнерів. Перевірка цілісності контейнерів полягає в розрахунку значень контрольної суми стегано-контейнерів,знаходженні хеш-функції стегано-контейнерів та зміні частот стегано-контейнерів. Етап застосування атаки полягає в додаванні адитивного гауссового білого шуму до стегано-контейнерів з метою їх спотворення. Потім знову розраховуються показники цілісності та спотврення для порівняння із значеннями до застосування атаки. Атака здійснюється з метою перевірки ефективності розробленої модифікації алгоритму.

Щоб оцінити продуктивність розробленої модифікації методу, до стегано-контейнеру додають адитивний гауссовий білий шум (AWGN) з різними значеннями дисперсії, перш ніж витягати таємне повідомлення, де тоді значення пікового сигналу до шумового співвідношення (PSNR) обчислюються та порівнюються з результатами, отриманими до додавання цього шуму.

3.5.1 Підготовка контейнеру та секретного повідомлення

Вхідні дані у проведеному дослілженні – файли контейнери та секретне повідомлення це аудіо файли MP3. На цьому кроці контейнер спочатку перетворюється з десяткового формату даних в двійковий.

Після підготовки контейнеру секретне повідомлення підготовлюється до процесу вбудовування в файл контейнер. Значення звукового сигналу секретного повідомлення перетворюються в позитивні значення, а потім перетворюється з десяткового формату даних в двійковий. Після цього іде етап перевірки, чи довжина секретного повідомлення менша, ніж довжина файлу контейнеру. Якщо довжина більша – обчислення зупиняються негайно. Якщо аудіофайл є монозвуком створюється вектор одного стовпця, а якщо стереозвук - матриця подвійного стовпця – лівий і правий канал, і потім робота продовжується з середнім значенням цих стовпців.

Далі йде етап перевірки, чи є швидкість передачі даних (Кбіт/сек) секретного повідомлення менше, ніж швидкість передачі даних файлу контейнеру. Файл контейнер має бути придатним для вкраплення секретного повідомлення у форматі

розміру. Якщо файл контейнер не є придатним – розрахунок зупиняється негайно, інакше – виконується наступний етап приховування даних.

3.5.2 Вкраплення секретоного повідомлення

При проведенні комплексного дослідження, секретне повідомлення приховується 4 способами: традиційні 4-LSB, 2-LSB, 1-LSB та розроблена модифікація.

Для традиційної техніки, в кожному з ітерацій циклу, вибраний байт змінюється за допомогою такої логіки:

- якщо використовується 4-LSB, то біти з 2-го до 5-го замінюються першими доступними 4 бітами в секретному повідомленні;
- якщо використовується 2-LSB, то біти 2-го - 3-го замінюються першими доступними бітами в секретному повідомленні;
- якщо використовується 1-LSB, тільки другий біт замінюється першим біт, доступним у секретному повідомленні.

Для розробленої модифікаї в кожному з циклів ітерацій біти приховані наступним чином:

- 1 біт приховується у першому байті;
- 2 біти приховується в другому байті;
- 2 біти приховується в третьому байті;
- 1 біт приховується у четвертому байті.

Після цього модифікований байт перетворюється назад з двійкового на десятковий, щоб створити стегано-об'єкт.

3.5.3 Оцінка спотворення вхідного файлу

На цьому етапі розраховується коефіцієнт пікового сигналу до шумового співвідношення (PSNR) та середня квадратична похибка (MSE). Обидва відображають дві метрики помилок, які використовуються для порівняння якості обкладинки. PSNR та MSE можна обчислити за допомогою наступних формул, відповідно:

$$\mathrm{MSE} = \frac{1}{\mathrm{N}}\sum_{\mathrm{i}=1}^{\mathrm{N}}(\mathrm{X(i)} - \mathrm{Y(i)})^2$$

$$\mathrm{PSNR} = 10\lg\frac{(\mathrm{MAX})^2}{\mathrm{MSE}}$$

де X – оригінальний об'єкт, Y - це стего-об'єкт, N - розмір обкладинки, MAX – максимальне значення амплітуди вхідного аудіо файлу.

3.5.4 Перевірка цілісності контейнерів

На цьому етапі застосовуються різні методи обробки, коли кожен метод, кодова книга зберігається і порівнюється пізніше з процесом вилучення.

На цьому етапі з метою порівняння стегано-контейнерів з вхідними файлами пропонується розрахунок наступних показників:

- значення контрольної суми стегано-контейнеру та вхідного файлу, потім рахуємо значення подібності даних, у відсотках;
- знаходження хеш-функції стегано-контейнерів та вхідних даних, і так само, у відсотках, рахуємо наскільки два файли подібні між собою;
- розраховується зміна частот у відсотках секретного повідомлення, витягнутого зі стегано-контейнера відносно вхідного секретного повідомлення.

3.5.5 Застосування атаки

Щоб оцінити продуктивність розробленого методу, перед етапом вилучення секретного повідомлення до стегано-контейнеру додають адативний гауссовий білий шум (AWGN) з різними значеннями дисперсії і тоді значення пікового сигналу до шумового співвідношення (PSNR) обчислюються та порівнюються з результатами, отриманими до додавання цього шуму.

Висновки до розділу

В межах даного розділу було оглянуто змістовну та математичну постановки задачі. Також було обгрунтовано вибір існуючого алгоритму для проведення модифікації.

Покроково описано етапи проведення дослідження, та представлено набір вхідних даних, який буде використаний в якості секретного повідомлення для проведення дослідження.

Описано суть розробленої модифікації та етап перевірки її ефективності відносно вже існуючих алгоритмів аудіо стеганографії. Результати експериментів та демонстрація роботи розробленої модифікації наведено та описано в наступному розділі.

4 Опис програмного продукту та результати дослідження

4.1 Засоби розробки

При створенні програмного продукту були використані такі засоби для програмування на мові C#, як Microsoft Visual Studio 2017 та Windows Forms.

C# проста у використанні, та водночас повноцінна мова програмування, що надає багато засобів для структурування і підтримки великих програм та рішень. Вона краще за C/C++ обробляє помилки, і, будучи мовою високого рівня, має вбудовані типи даних високого рівня, такі як гнучкі масиви, списки і словники, ефективна реалізація яких на C/C++ потребує значних витрат часу. Також для розширення функціональності можна використовувати готові бібліотеки, які отримуються напряму в середу розробки через вбудований у Visual Studio 2017 менеджер пакетів NuGet Package Manager.

C# дозволяє розбивати програми на модулі, що потім можуть бути використані в інших програмах. При наявності великих рішень зазвичай програма розбивається на окремі проекти, які відповідають за певний клас схожих за направленістю задач, це робиться для легшого орієнтування у рішенні та структурування рішень. C# поставляється з великою кількістю стандартних бібліотек, які можна використовувати, як основу для нових програм або як приклади при вивченні мови. Стандартні модулі надають засоби для роботи з файлами, системними викликами, мережними з'єднаннями і навіть інтерфейсами до різних графічних бібліотек.

C# - інтерпретована мова, що дозволяє заощадити значну кількість часу, що зазвичай витрачається на компоновку та компіляцію рішення. Інтерпретатор можна використовувати інтерактивно, що дозволяє експериментувати з можливостями мови. C# дозволяє писати зручні для читання програми завдяки загальноприйнятим узгодженням щодо написання коду та назв полів різних типів. Програми, написані мовою C#, звичайно значно коротші ніж їхні еквіваленти на C/C++ з декількох причин:

- типи даних високого рівня дозволять Вам виразити складні операції однією інструкцією;
- наявність новіших методів;
- широкий вибір методів та структур.

Синтаксис C# близький до C++ і Java. Мова має строгу статичну типізацію, підтримує поліморфізм, наслідування, перевантаження операторів, інкапсуляцію, закриття методів, вказівники на функції та члени класів, атрибути, події, властивості, делегати, винятки, коментарі у форматі XML. Перейнявши багато чого від своїх попередників — мов C++, Delphi і Smalltalk — C#, спираючись на практику їхнього використання, виключає деякі моделі, що зарекомендували себе як проблематичні при розробці програмних систем, наприклад множинне спадкування класів (на відміну від C++) [8].

Windows Forms дозволяє розробляти інтелектуальні клієнти. Інтелектуальний клієнт - це програма з повнофункціональним графічним інтерфейсом, просте в розгортанні і оновленні, здатне працювати при наявності або відсутності підключення до Інтернету і використовує більш безпечний доступ до ресурсів на локальному комп'ютері в порівнянні з традиційними додатками Windows.

Windows Forms - це технологія інтелектуальних клієнтів для .NET Framework. Вона являє собою набір керованих бібліотек, що спрощують виконання стандартних завдань, таких як читання з файлової системи і запис в неї. При використанні середовища розробки, як Visual Studio, можна створювати інтелектуальні клієнтські програми Windows Forms, які відображають відомості, запитують введення від користувачів і обмінюються даними з віддаленими комп'ютерами по мережі.

У Windows Forms, форма - це візуальна поверхня, на якій виводиться інформація для користувача. Зазвичай додаток Windows Forms будується шляхом приміщення елементів управління на форму і написання коду для реагування на дії користувача, такі як клацання миші або натискання клавіш. Елемент управління - це окремий елемент призначеного для користувача інтерфейсу, призначений для відображення або введення даних.

При виконанні користувачем якої-небудь дії з формою або з одним з елементів управління створюється подія. Додаток реагує на ці події за допомогою коду і обробляє події при їх виникненні.

Windows Forms включає широкий набір елементів управління, які можна додавати на форми: текстові поля, кнопки, списки, що розкриваються, перемикачі та навіть веб-сторінки. Якщо існуючий елемент управління не задовольняє потребам, в Windows Forms можна створювати власні елементи управління.

До складу Windows Forms входять багатофункціональні елементи призначені для користувача інтерфейсу, що дозволяють відтворювати можливості таких складних додатків, як Microsoft Office. Використовуючи необхідні елементи управління, можна створювати панелі інструментів і меню, що містять текст і малюнки, та інші елементи управління, такі як текстові поля і поля зі списками.

За допомогою Visual Studio можна легко створювати додатки Windows Forms. Досить виділити елемент керування курсором і помістити його в потрібне місце на формі. Для подолання труднощів, пов'язаних з вирівнюванням елементів управління, конструктор надає такі додаткові елементи, як лінії сітки і лінії прив'язки. За допомогою Visual Studio або компіляції з командного рядка, можна використовувати елементи управління для створення складних макетів форм за менший час.

У багатьох додатках потрібно відображати дані з бази даних, XML-файла, веб-служби XML або іншого джерела даних. Windows Forms надає гнучкий елемент управління для відображення таких табличних даних в традиційному форматі рядків і стовпців так, що кожен фрагмент даних займає свою власну клітинку. За його допомогою можна, налаштувати зовнішній вигляд окремих осередків, зафіксувати рядки і стовпці на своєму місці, а також забезпечити відображення складних елементів управління всередині осередків.

За допомогою Windows Forms можна легко створювати елементи управління з прив'язкою до даних. Створювати елементи управління з прив'язкою до даних можна шляхом перетягування об'єктів з допоміжного вікна в форми проекту. Також

можна пов'язувати існуючі елементи управління з даними, перетягуючи об'єкти в існуючі елементи управління.

Інший тип прив'язки до даних в формах Windows Forms - це параметри. Більшість інтелектуальних клієнтських додатків повинні зберігати деякі відомості про свій стан під час виконання, такі як відомі розміри форм, а також зберігати призначені для користувача дані, наприклад місце збереження файлів за замовчуванням. Додаток Windows Forms надає простий спосіб зберігання обох типів відомостей на клієнтському комп'ютері. Після визначення ці параметри за допомогою Visual Studio або редактора коду, зберігаються в XML-файлі і автоматично зчитуються назад в пам'ять під час виконання.

4.2 Архітектура програмного забезпечення

Схема структурна варіантів використання. Схема структурна варіантів використання наведена в додатку А.

Схема структурна діяльності. Схема структурна діяльності у додатку показує основні можливі процеси роботи програмного продукту. Схема структурна діяльності наведена в додатку А.

Схема структурна послідовності. Схема структурна послідовності охоплює процес приховування даних в аудіо файлі. Схема структурна послідовності наведена у додатку А.

4.3 Демонстрація роботи продукту

В рамках даної роботи, розроблено програминй застосунок. На рисунку 4.1 показано початкову форму програмного продукту. На даному етапі користувачу потрібно обрати тип роботи програми – комплексне тестування якості приховування даних чи одноразове, тобто для одного аудіо файлу.

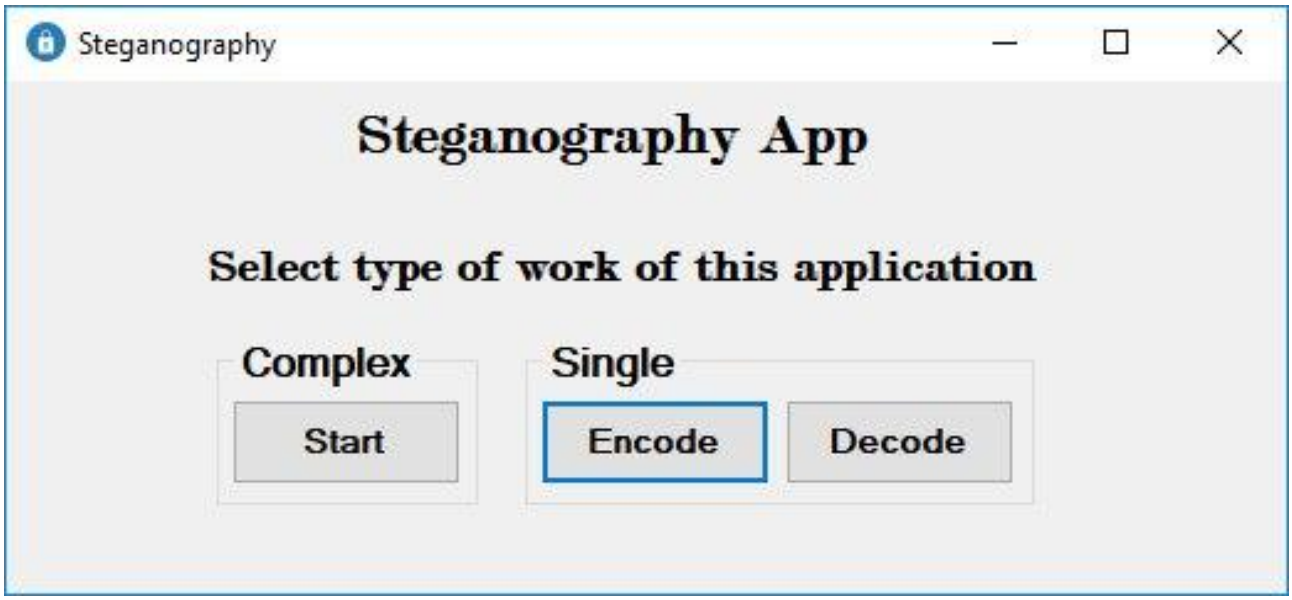

Рисунок 4.1 – Початкова форма програмного продукту

На рисунку 4.2 показано наступну форму – після вибору варіанту приховування даних для одного файлу.

Рисунок 4.2 – Форма кодування даних для одного файлу

На даному етапі потрібно обрати аудіо файл, в який і буде приховано секретне повідомлення. Також, потрібно обрати метод, яким буде закодовано повідомлення

до аудіо контейнера та ввести секретне повідомлення. Програмний продукт дозволяє обрати одразу декілька методів, і тоді, в рузультаті кодування буде створено декілька стеганоконтейнерів.

На рисунку 4.3 показано результат кодування. На даному етапі користувач може прослухати стегано-контейнер, щоб спробувати відчути на власний слух чи з’явилися помітні зміни аудіо контейнеру. Також розраховуються коефіцієнти – відношення пікового сигналу відносно шумового співвідношення; подібність даних у відсотках між значенням контрольної суми стегано-контейнеру та вхідного файлу; подібність даних у відсотках між хеш-функцією стегано-контейнеру та вхідних даних, у відсотках; зміну частот у відсотках секретного повідомлення, витягнутого зі стегано-контейнера відносно вхідного секретного повідомлення.

Корстувач може спотворити отриманий стегано-контейнер, додавши до нього адитивний гауссовий білий шум з певним коефіцієнтом дисперсії.

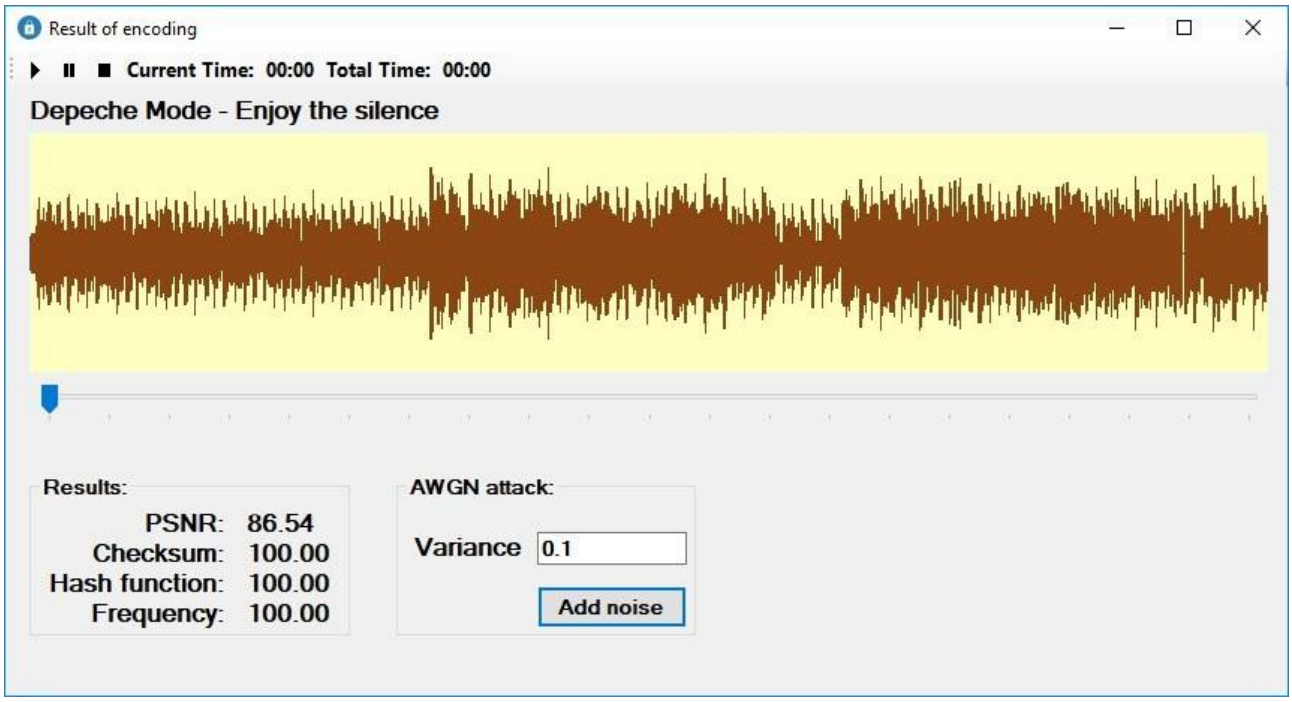

Рисунок 4.3 – Форма з результатами приховування даних

Вихідні дані після кодування даних показані на рисунку 4.4.

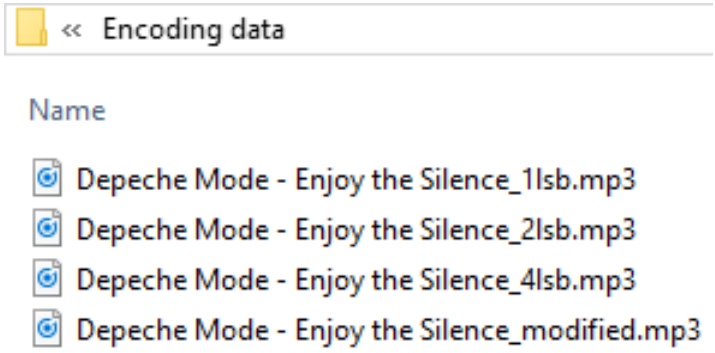

Рисунок 4.4 – Вихідні дані після кодування інформації

Після додавання атаки на стегано-контейнер, отримані коефіцієнти перераховуються та додається ще один стегано-контейнер. Результат показано на рисунку 4.5

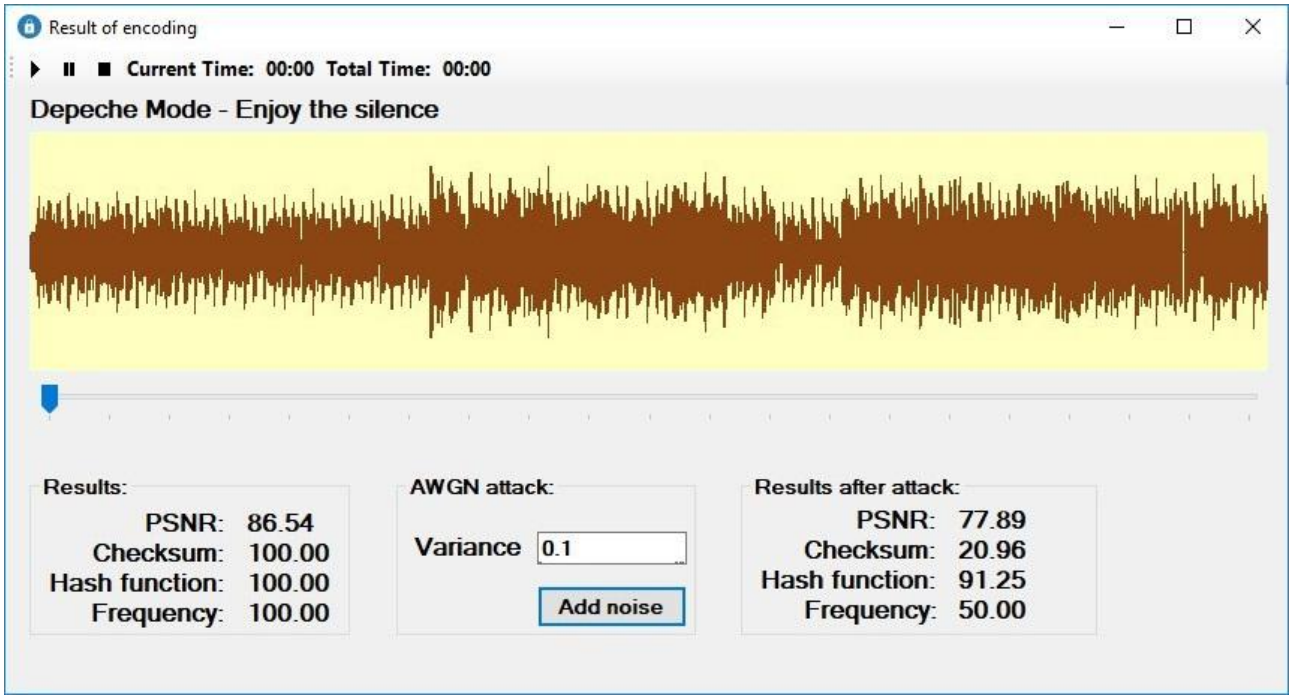

Рисунок 4.5 – Видозмінена форма результату кодування після додавання атаки на стегано-контейнер.

Додані вихідні дані після здійснення атаки на стегано контейнер показані на рисунку 4.6.

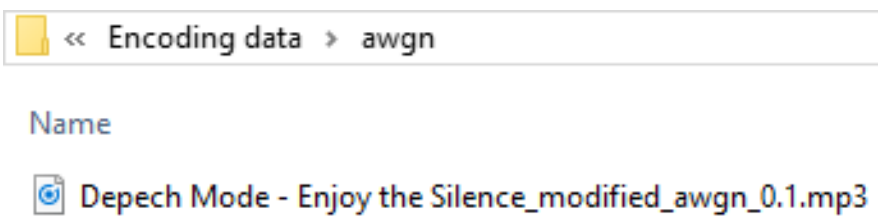

Рисунок 4.6 – Вихідні дані після здійснення атаки на стегано-контейнер

Повертаючись до початкової форми, показаної на рисунку 4.1, оберемо декодування даних. Наступна форма, декодування даних показана на рисунку 4.7.

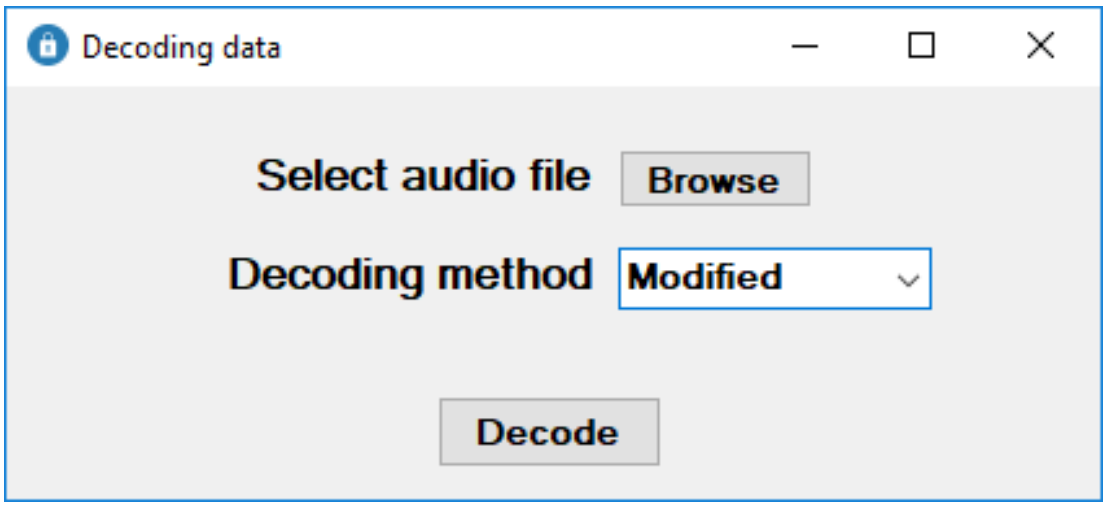

Рисунок 4.7 – Форма декодування даних зі стегано-котейнеру

На даному етапі потрібно обрати стегано-контейнер із вкрапленим секретним повідомленням та обрати метод, яким було закодоване секретне повідомлення. Результат показано на рисунку 4.8.

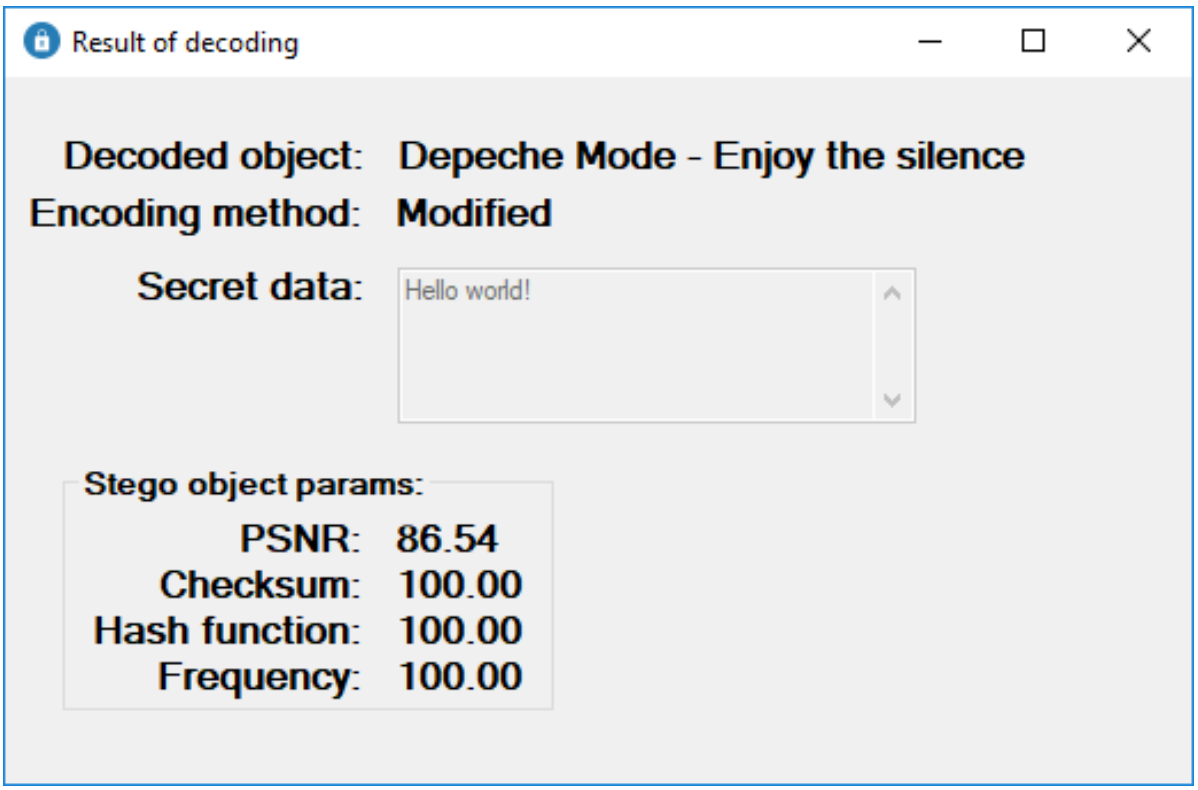

Рисунок 4.8 – Результат декодування даних зі стегано-контейнеру

На формі, продемонстрованій вище, наведені назва стегано-контейнеру, з якого було отримане секретне повідомлення, саме секретне повідомлення, метод, яким секретне повідомлення було вкраплене в стегано-контейнер та параметри цього контейнеру.

Обравши на початковій формі програмного продутку варінт комплексного дослідження, отримаємо форму показану на рисунку 4.9.

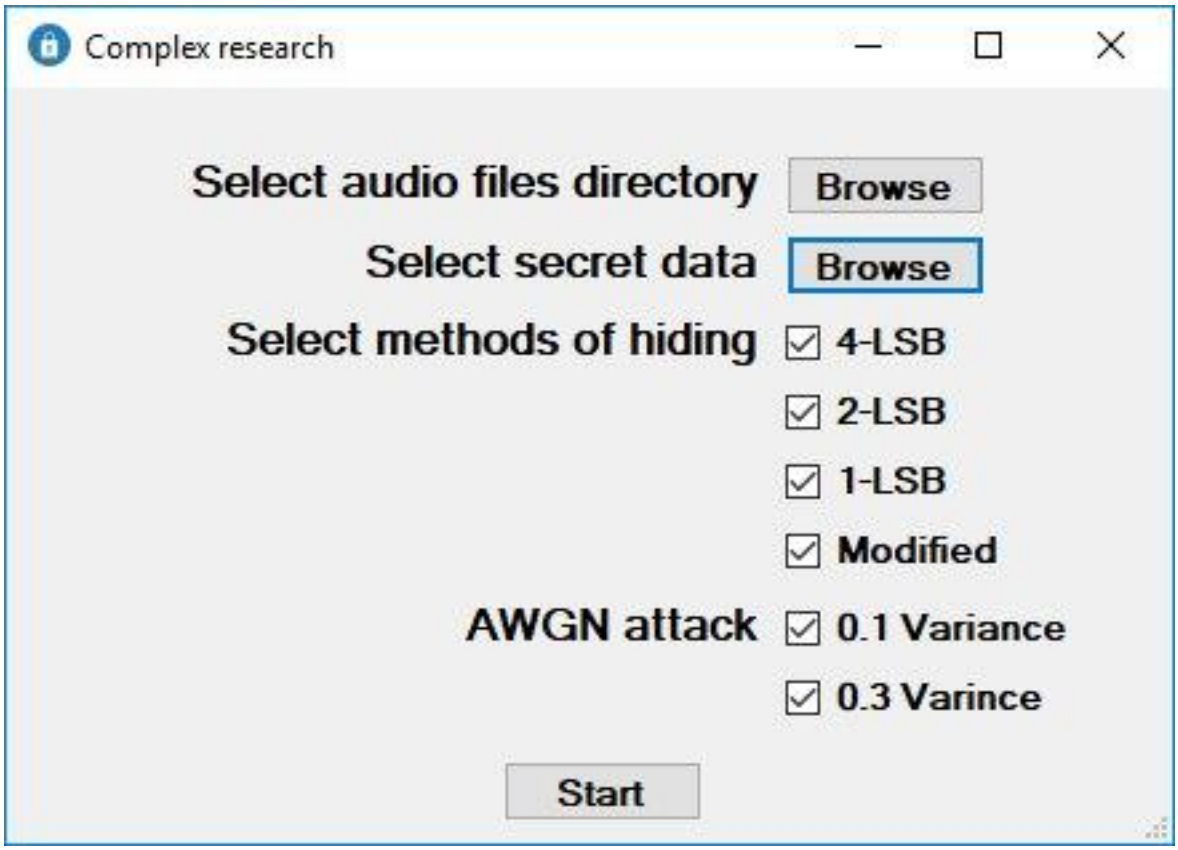

Рисунок 4.9 – Форма налаштування комплексного дослідження

По-перше, потрібно обрати папку з вхідними даними – набір аудіофайлів, в які буде вкпраплено приховані дані. Наступне, обрати секретні дані – в своїх дослідженнях секретними даними виступає також аудіо файл, але з меншим бітрейтом – 96 кбіт/сек. Обрати бажані методи вкраплення інформації, та задати параметри атаки на отримані стегано-контейнери. Після початку даного дослідження, з’являється наступна форма, показана на рисунку 4.10.

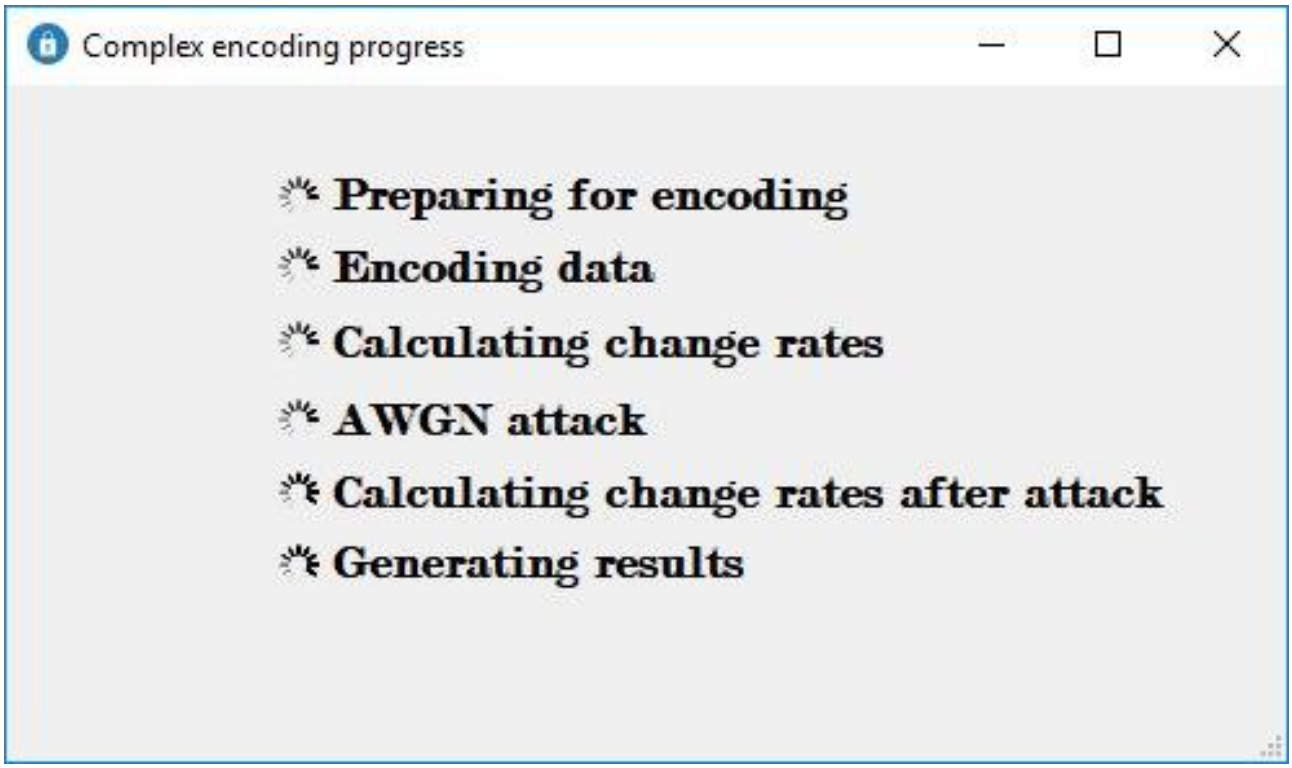

Рисунок 4.10 – Форма налаштування комплексного дослідження

На даній формі показано процес проведнння дослідження. Всі результати дослідження формуються та записуються до Excel файлу. Приклад результатів показано на рисунку 4.11.

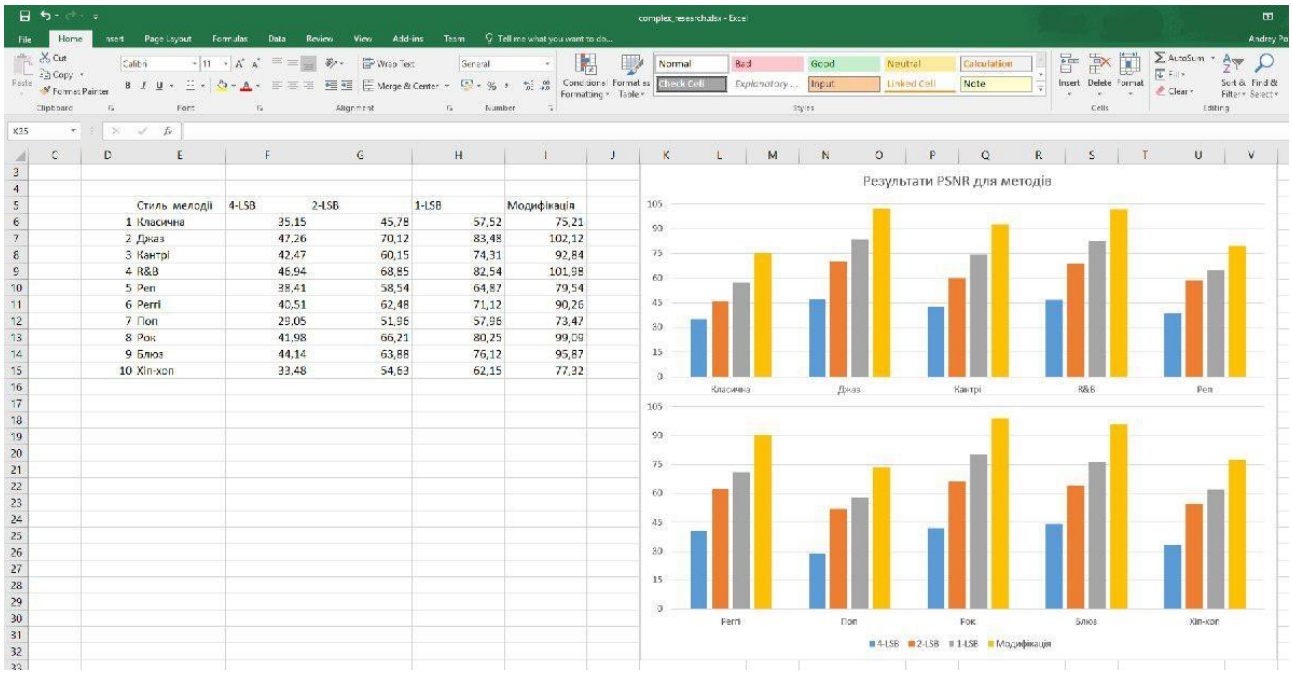

Рисунок 4.11 – Вихідні результати комплексного дослідження

4.4. Результати дослідження

Проведена робота в даному дослідженні спрямована на ефективну модифікацію існуючого методу аудіо стеганографії, а саме – методу найменш значущого біту (LSB). Крім того, пропонується ефективний спосіб перевірки достовірності отриманих результатів, за допомогою розробленого програмного продукту. Також, програмний застосунок надає зручні вихідні дані, із всіма необхідними розрахунками та діаграмами.

В проведеному дослідженні, секретним повідомленням, яке вкраплювалось у вхідні дані, є MP3 аудіо файл. Для порівняння отриманих результатів використовуючи розроблену модифікацію алгоритму найменш значущого біту, також проведені процеси приховування даних традиційними методами найменш значущого. Аудіо повідомлення вбудовується в вхідні файли, використовуючи три традиційні методи LSB: 4-LSB, 2-LSB і 1-LSB та розроблену модифікацію, щоб порівняти їх ефективність.

4.4.1 Результати процесу приховування даних

У цій частині секретне повідомлення приховане в усіх вхідних файлах, використовуючи як модифікований алгоритм, так і традиційні методи LSB.

В цьому дослідженні, вхідними даними виступають аудіо MP3 файли, по 20 файлів кожного із наступних стилів музики: Класична, Джаз, Кантрі, R&B, Реп, Реггі, Поп, Рок, Блюз, Хіп-хоп.

Результуючі значення PSNR після вставки секретного повідомлення, розміром близько 1 Мбайт для 10 різних стилів музики. Секретне повідомлення приховане за допомогою розробленеї модифікації та трьох традиційних методів LSB – 4-LSB, 2-LSB і 1-LSB. Результати показані в таблиці 4.1 та на рисунку 4.12.

Таблиця 4.1 – Результуючі значення PSNR для обраних методів

Стиль мелодії	**PSNR 4-LSB, Дб**	**PSNR 4-LSB, Дб**	**PSNR 4-LSB, Дб**	**PSNR модифікації, Дб**
Класична	35,15	45,78	57,52	75,21
Джаз	47,26	70,12	83,48	102,12
Кантрі	42,47	60,15	74,31	92,84

Продовження таблиці 4.1.

R&B	46,94	68,85	82,54	101,98
Реп	38,41	58,54	64,87	79,54
Реггі	40,51	62,48	71,12	90,26
Поп	29,05	51,96	57,96	73,47
Рок	41,98	66,21	80,25	99,09
Блюз	44,14	63,88	76,12	95,87
Хіп-хоп	33,48	54,63	62,15	77,32

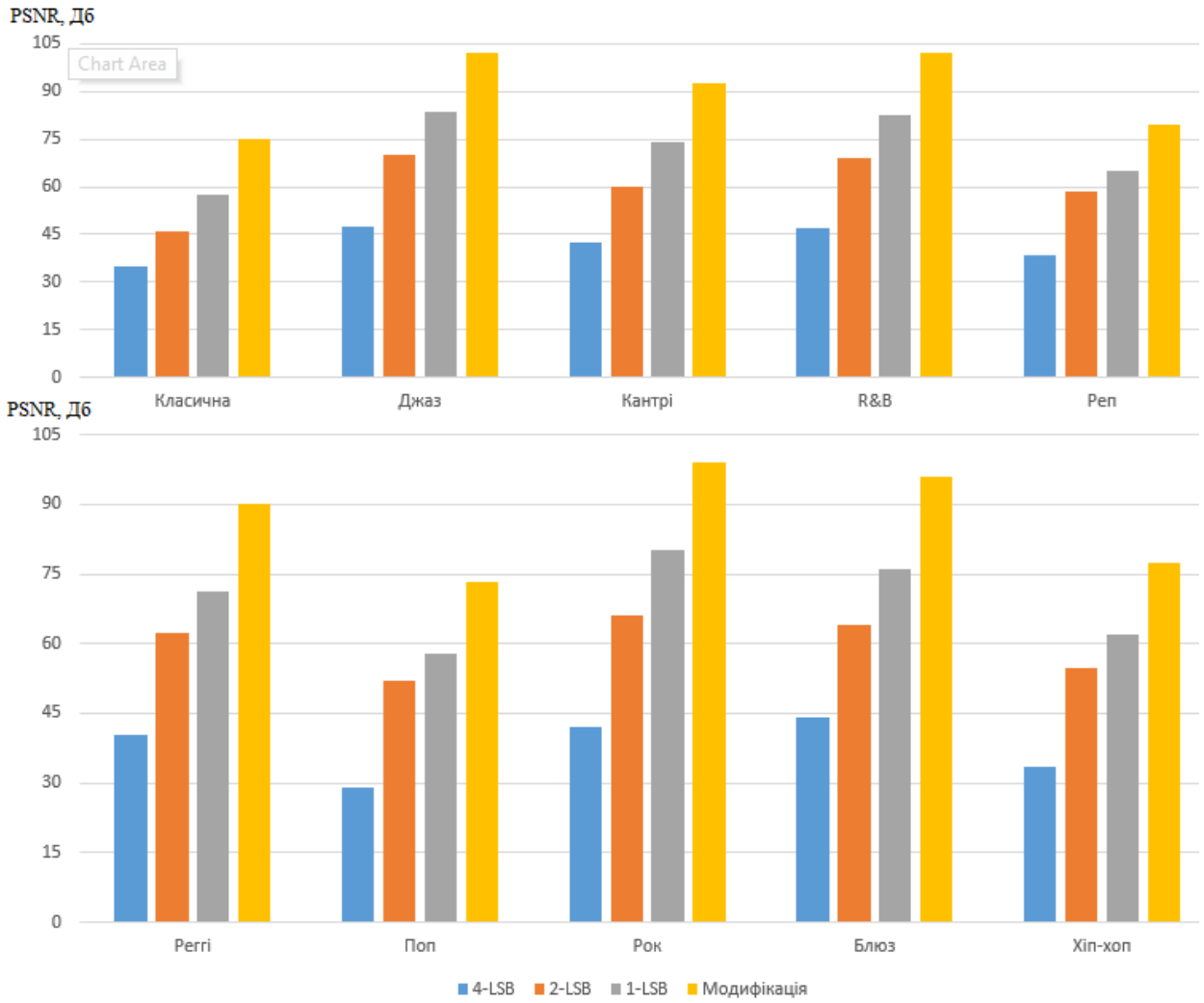

Рисунок 4.12 – Результуючі значення PSNR для обраних методів

Можна чітко бачити, що результати PSNR пропонованого методу краще, ніж традиційні LSB для всіх жанрів. Як показано вище, Джаз пропонує найвищий PSNR, оскільки він є одним з MP3-файлів, який містить більш високий рівень шуму, ніж інші звукові файли. Таким чином, він пропонує високий PSNR.

У наведеній нижче таблиці 4.2 показаний відсоток покращення між поточним методом та традиційними методами для попередніх вхідних даних на основі отриманих даних на попередньому кроці.

Таблиця 4.2 – Перевага модифікованого алгоритму відносно традиційних

Стиль мелодії	**Відношення PSNR 4-LSB до модифікації, %**	**Відношення PSNR 2-LSB до модифікації, %**	**Відношення PSNR 1-LSB до модифікації, %**
Класична	53,26	39,13	23,52
Джаз	53,72	31,34	18,25
Кантрі	54,25	35,21	19,96
R&B	53,97	32,49	19,06
Реп	51,71	26,40	18,44
Реггі	55,12	30,78	21,21
Поп	60,46	29,28	21,11
Рок	57,63	33,18	19,01
Блюз	53,96	33,37	20,60
Хіп-хоп	56,70	29,35	19,62

4.4.2 Результати додавання AWGN-атаки

У цій частині застосовується один з видів атаки – адитивний гауссовий білий шум (AWGN) додається до стегано-контенерів, тобто для всіх вихідних даних, які були отримані модифікованим алгоритмом, перш ніж витягати з них секретне повідомлення. Потім, повідомлення витягується та здійнюється порівняння його оцінки PSNR зі значенням цієї оцінки стегано-контейнерів до застосування атаки.

Атака AWGN додана до всіх стегано-контейнерів, які отримали секретні дані розробленим модифікофаним алгоритмом з різними значеннями шумової дисперсії. Таблиця 4.3 показує отримані значення PSNR для стегано-контейнерів після атаки зі значенням дисперсії 0,1 біт/сек/Гц для всієї смуги кожного стегано-контейнеру.

Таблиця 4.3 – Результати після атаки до стегано-контейнерів зі значенням дисперсії 0.1

Стиль мелодії	**PSNR до атаки, Дб**	**Дисперсія, біт/сек/Гц**	**PSNR після атаки, Дб**	**Погіршення, %**
Класична	75,21	0,1	69,76	7,25
Джаз	102,12	0,1	95,33	6,65
Кантрі	92,84	0,1	86,83	6,47
R&B	101,98	0,1	97,92	3,98
Реп	79,54	0,1	75,32	5,31
Реггі	90,26	0,1	85,56	5,21
Поп	73,47	0,1	70,52	4,02
Рок	99,09	0,1	93,82	5,32
Блюз	95,87	0,1	92,56	3,45
Хіп-хоп	77,32	0,1	73,57	4,85

У таблиці 4.4 показані досягнуті значення PSNR для стегано-контейнерів після атаки зі значенням дисперсії 0,3 біт/сек/Гц для всієї смуги кожного стегано-контейнеру.

Таблиця 4.4 – Результати після атаки до стегано-контейнерів зі значенням дисперсії 0.3

Стиль мелодії	**PSNR до атаки, Дб**	**Дисперсія, біт/сек/Гц**	**PSNR після атаки, Дб**	**Погіршення, %**
Класична	75,21	0,3	65,92	12,35
Джаз	102,12	0,3	92,58	9,34
Кантрі	92,84	0,3	83,33	10,24
R&B	101,98	0,3	94,70	7,14
Реп	79,54	0,3	72,41	8,96
Реггі	90,26	0,3	81,61	9,58
Поп	73,47	0,3	67,88	7,61
Рок	99,09	0,3	89,60	9,58
Блюз	95,87	0,3	89,19	6,97
Хіп-хоп	77,32	0,3	71,05	8,11

Можна зробити висновок про наявність очевидної деградації значення PSNR після додавання атаки AWGN. Як показано в таблицях вище, деградація у значеннях PSNR збільшується із збільшенням значення дисперсії шумів.

Отримані результати значень PSNR після додавання атаки AWGN з шумовою дисперсією 0,1 показані на рисунку 4.13.

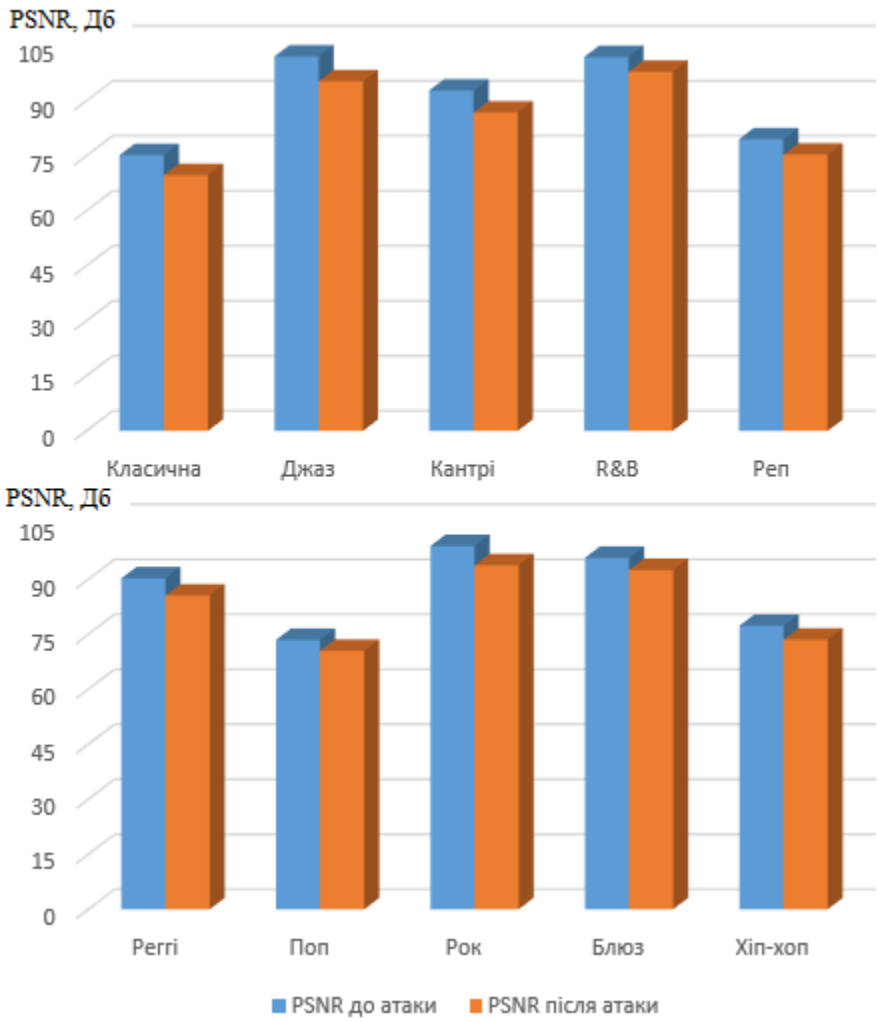

Рисунок 4.13 – Порівняння значень PSNR до і після додавання атаки зі значенням шумової дисперсії 0,1 біт/сек/Гц

Отримані результати значень PSNR після додавання атаки AWGN з шумовою дисперсією 0,3 показані на рисунку 4.14.

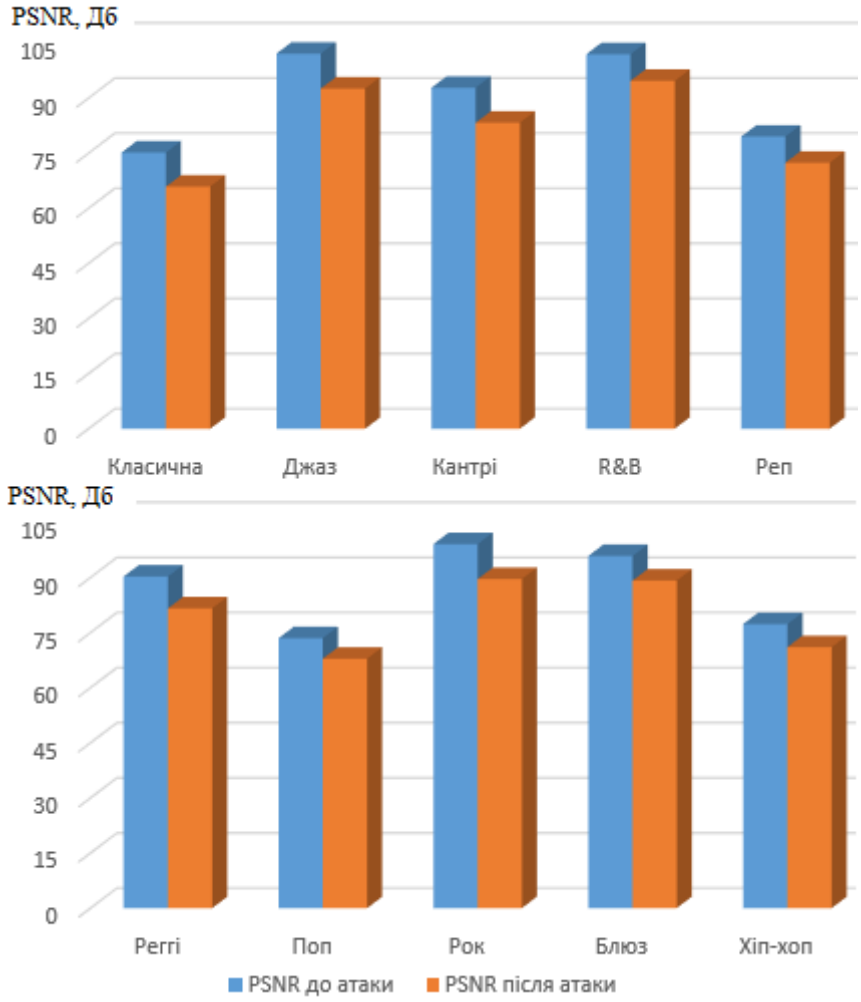

Рисунок 4.14 – Порівняння значень PSNR до і після додавання атаки зі значенням шумової дисперсії 0,3 біт/сек/Гц

4.4.3. Результати розрахунку показників цілісності

Для порівняння стегано-контейнерів з вхідними файлами, програмний застосунок розраховує наступні показники: значення контрольної суми стегано-контейнеру та вхідного файлу, і видає значення подібності даних, у відсотках; розраховує хеш-функції стегано-контейнерів та вхідних даних, і так само, показує у відсотках, наскільки два файли подібні між собою; зміна частот показує у відсотках зміну секретного повідомлення, витягнутого зі стегано-контейнера відносно вхідного секретного повідомлення.

У наведеній нижче таблиці 4.6 представлені досягнуті відсотоки для вихідних даних отриманих модифікованим алгоритмом відносно вхідних даних, до застосування атаки на них.

Таблиця 4.6 – Результати показників цілісності для модифікації алгоритму

Стиль мелодії	**Контрольна сума, %**	**Хеш-функція, %**	**Зміна частот, %**
Класична	100	100	100
Джаз	100	100	100
Кантрі	100	100	100
R&B	100	100	100
Реп	100	100	100
Реггі	100	100	100
Поп	100	100	100
Рок	100	100	100
Блюз	100	100	100
Хіп-хоп	100	100	100

Як показано в таблиці вище, робота розробленої модифікації алгоритму не спотворює вихідні дані, оскільки всі показники оцінки якості отриманих даних мають значення 100%, для всіх стилів музики. Ці результати отримані без застосування атаки на стегано-контейнери.

Далі, йде процес атаки, додавання адитивного гауссового білого шуму (AWGN) до стегано-контейнерів, отриманих в результаті роботи розробленої модифікації алгоритму. Результати, отримані у процесі порівняння стегано-контейнерів до атаки та після за вище описаними критеріями показано в таблиці 4.7.

Таблиця 4.7 – Результати показників цілісності після застосування атаки

Стиль мелодії	**Контрольна сума, %**	**Хеш-функція, %**	**Зміна частот, %**
Класична	21,42	92,14	50
Джаз	21,25	91,88	50
Кантрі	21,71	92,54	50
R&B	21,14	92,17	50
Реп	20,84	91,25	50
Реггі	20,54	90,28	50
Поп	20,65	90,77	50
Рок	21,21	91,25	50
Блюз	20,25	90,17	50

Продовження таблиці 4.7.

Хіп-хоп	21,17	90,14	50

Як показано в таблиці вище, найкращий відсоток подібності стегано-контейнерів до атаки та після, демонструє перевірка хеш-функції, тоді як мінімальні досягнуті результати є для значення контрольної суми. Графічне відображення отриманих результатів, з таблиці 4.7 продемонстровано на рисунку 4.15.

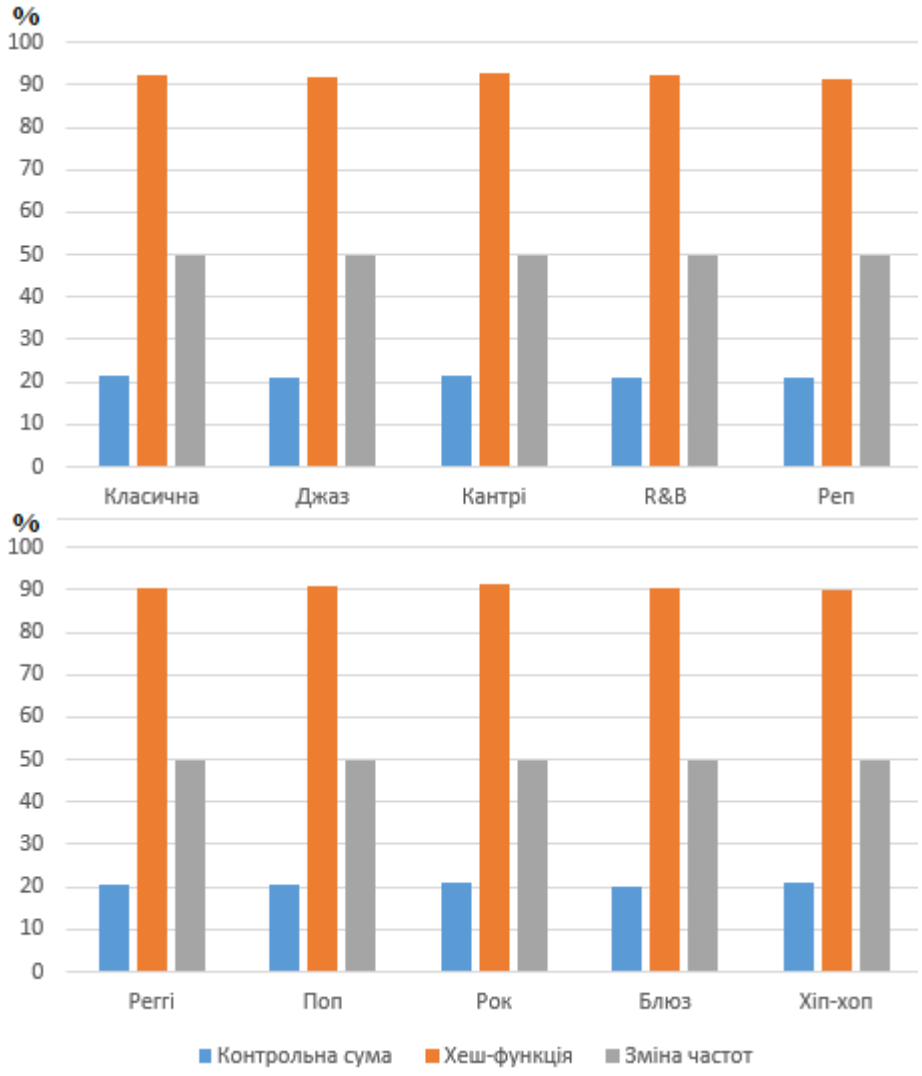

Рисунок 4.15 – Показники цілісності стегано-контейнерів після застосування атаки

4.5 Результати розрахунку показників цілісності для 1-LSB методу

У цьому випадку атака застосовується до стегано-контейнерів отриманих методом традиційного 1-LSB.

У таблиці 4.8 показані досягнуті значення PSNR для стегано-контейнерів після атаки зі значенням дисперсії 0,1 біт/сек/Гц для всієї смуги кожного стегано-контейнеру.

Таблиця 4.8 – Результати після атаки до стегано-контейнерів зі значенням дисперсії 0.1

Стиль мелодії	**PSNR до атаки, Дб**	**Дисперсія, біт/сек/Гц**	**PSNR після атаки, Дб**	**Погіршення, %**
Класична	57,52	0,1	48,34	15,96
Джаз	83,48	0,1	71,15	14,77
Кантрі	74,31	0,1	66,14	10,99
R&B	82,54	0,1	72,58	12,07
Реп	64,87	0,1	53,74	17,16
Реггі	71,12	0,1	60,59	14,81
Поп	57,96	0,1	49,15	15,20
Рок	80,25	0,1	69,54	13,35
Блюз	76,12	0,1	64,97	14,65
Хіп-хоп	62,15	0,1	50,85	18,18

Наведені вище таблиці показують, що після атаки, тобто додавання адитивного гауссового білого шуму (AWGN) до стегано-контейнерів отрманих методом 1-LSB, спостерігається чітка деградація значень PSNR. Крім того, очевидно, що деградація PSNR набагато гірша порівняно з розробленою модифікацією алгоритму.

У таблиці 4.9 показані результати, отримані у процесі порівняння стегано-контейнерів до атаки та після для техніки 1-LSB.

Таблиця 4.9 – Результати показників цілісності після застосування атаки для 1-LSB.

Стиль мелодії	**Контрольна сума, %**	**Хеш-функція, %**	**Зміна частот, %**
Класична	17,58	82,14	44,47
Джаз	19,58	86,88	44,47
Кантрі	18,25	80,54	44,47
R&B	20,21	79,17	44,47
Реп	19,28	85,25	44,47
Реггі	18,17	88,28	44,47

Поп	18,25	84,77	44,47

Продовження таблиці 4.9.

Рок	17,85	89,25	44,47
Блюз	20,85	83,17	44,47
Хіп-хоп	19,57	84,14	44,47

Як показано в таблиці вище, технологія 1-LSB пропонує гірші значення показників цілісності стегано-контейнерів після застосування атаки на них, в порівнянні з розробленою модифікацією алгоритму.

Висновки до розділу

У межах розділу здійснено розробку програмного застосунку для вирішення поставленої задачі. Описано основні модулі програми, архітектуру програмного застосунку та здійснено демонстрацію роботи застосунку.

Під час демонстрації роботи збоїв та недоліків не виявлено, що говорить про високу якість розробки та можливість впровадження у роботу за потребою.

Проведено комплексне дослідження роботи модифікованого алгоритму, використовуючи розроблений програмний продукт. Проаналізовано результати досліджень в порівнянні з традиційними алгоритмами.

ВИСНОВКИ

У даній магістерській дисертації було розроблено модифікований алгоритм найменшого значного біту (LSB). Дана модифікація показала кращі результати ніж традиційні методи найменш значущого біту, також демонструє вищий рівень стійкості до атаки з додаванням адитивного гауссового білого шуму. Мовою реалізації програмної частини є C#.

В дисертації було проаналізовано предметну область та розглянуто існуючі методи аудіо стеганографії, проаналізовано їх переваги та недоліки, проведене їх порівняння. Було проведено аналіз зменшення внесення помітних змін до файлів контейнерів, та щодо збільшення стійкості контейнерів до атак. На основі проведеного аналізу було вирішено розробляти модифікацію саме методу найменш значущого біту через те що цей метод забезпечує більшу безпеку та є ефективним способом приховування секретної інформації від хакерів і відправлення в пункт призначення безпечним та невиявленим способом. Також, метод гарантує, що розмір файлу не змінюється навіть після кодування, і також підходить для будь-якого типу формату аудіофайлів. Також він дозволяє приховувати в файлах контейнерах набагото більший об'єм секретної інформації в порівнянні з іншими алгоритмами.

Задля перевірки ефективності розробленої модифікації, було проведено дослідження на аудіо файлах різних жанрів різного розміру. Також проведено один з видів атаки на ці контейнери щоб перевірити їх стійкість, в порівнянні з традиційними методами найменш значущого біту.

В рамках опису розробленої архітектури розробленого програмного продукту наведено схему структурну послідовності, схему структурну діяльності та схуму структурну варіантів використання, продемонстровано ітерацію комлексного дослідження, з додаванням атаки на контейнери, також надано детальний опис розробленого алгоритму. Також наведена інструкція з використання застосунку Наведено приклади атак на вихідні контейнери застосунку.

До результатів досліджень, додано їх графічна ілюстрація, та порівняльний аналіз з традиційним методом, також і для додавання атаки на стегано-контейнери, де видно, що розроблена модифікація показує кращі результати.

З огляду на вище наведене можна зробити висновок, що в результаті проведеної роботи було досягнуто поставлену мету.

ПЕРЕЛІК ПОСИЛАНЬ

1. Проблемы выявления скрытой передачи информации по сетям [Електронний ресурс] / Режим доступу: http://www.ipages.ru/index.php?ref_item_id=798&ref_dl=1.
2. Стеганография в XXI веке. Цели. Практическое применение. Актуальность [Електронний ресурс] / Режим доступу: https://habrahabr.ru/post/253045/
3. Грибунин В.Г., Оков И.Н., Туринцев И.В Цифровая сеганография [Текст] / Грибунин В.Г. // Москва: СОЛОН-Пресс, 2002 р. – 261 с.
4. Phitzman B. Information hiding terminology [Текст] Information Hiding: First Int. Workshop “InfoHiding’96” / Springer as Lecture Notes in Computing Science, 1996 р. – 350-374 с.
5. Михалевич В.С., Сергиенко И.В., Задирака В.К., Бабич М.Д. К вопросу оптимизации вычислений [Текст] / Кибернетика и системный анализ, 1994 р. – 65-74 с.
6. Чецов Н.Н. Статистические решающие правила и оптимальные выводы [Текст] / Ченцов Н.Н. // Москва: Наука, 1972 р. – 520 с.
7. Weinstein C.J. Roundoff noise in floating point fast Fourier transform computation [Текст] / IEEE Trans. Audio Elekroacoust, 1969 р. – 19 с., N 2. – 209-211 с.
8. Хлобыстов В.В., Задирака В.К. Об одном распределении, связанном с нормальным [Текст] / Вычислительная и прикладная математика, 1977 р. – Вып. 31 – 72-75 с.
9. Сергиенко И.В., Задирака В.К., Бабич М.Д., Березовский А.И., Бесараб П.Н., Людвиченко В.А. Компьютерные технологии решения задач прикладной и вычислительной математики с заданными значениями характеристик качества [Текст] / Кибернетика и системный анализ, 2006 р. – № 5 – 33-41 с.
10. Пугачев В.С. Теория случайных функций [Текст] / Пугачев В.С. // Москва: Физматгиз, 1960 р. – 883 с.
11. Сергиенко И.В., Задирака В.К., Бабич М.Д., Березовский А.И., Бесараб П.Н., Людвиченко В.А. О компьютерной технологии построения Т-эффективных

алгоритмов вычесления Ɛ-решений задач вычислительной и прикладной математики [Текст] / Кибернетика и системный анализ, 2002 р. – № 6 – 51-54 с.

12. Кошкина Н.В. Выявление Hide4PGP вложений в аудиосигналах [Текст] / Кошкина Н.В. // Международный научно-технический журнал «Проблемы управления и информатики», 2013 р. – № 3. – 151-153с.
13. Кошкіна Н.В. Стегоаналіз цифрових зображень із застосуванням контрольного вкраплення [Текст] / Кошкіна Н.В. // Матеріали 3 Міжнародної науково-технічної конференції «Захист інформації і безпека інформаційних систем», Львів. – 2014 р. – 98-100 с.
14. Кошкина Н.В. Стегоанализ бесключевых стеганосистем на основе атаки контрольным внедрением [Текст] / Кошкина Н.В. // Международный научно-технический журнал «Проблемы управления и информатики», 2014 р. – № 6. – 137-141с.
15. Литвин О.Н., Першина Ю.І. Reconstruction of 3-D objects with use interflation of function [Текст] / Conf. on Automation, Control, and Information Technology // Оброблення сигналів і зображеньта розпізнавання образів, Новосибирск. – 2005 р. – 274-276 с.
16. Яненко Н.Н. Вычислительный алгоритм [Текст] / Энциклопедия математики. – Т. 1. // Москва: Советская энциклопедия, 1977 р. – 826-827 с.
17. Воеводин В.В. Вычеслительные основы линейной алгебры [Текст] / Воеводин В.В. // Москва: Наука, 1977 р. – 303 с.
18. Виленкин Н.Я. Комбинаторика [Текст] / Виленкин Н.Я. // Москва: Наука, 1969 р. – 328 с.
19. Задирака В.К. О требованиях и параллельной обработке данных в спецпроцессоре БПФ [Текст] / Оптимизация алгоритмов и программного обеспечения ЭВМ // Киев: Институт кибернетики им. В.М. Глушкова АН УССР, 1985 р. – 10 с.
20. Обзор методов решений аудио стеганографии [Електронний ресурс] / Режим доступу: https://sibac.info/studconf/tech/xlii/54331.

21. Стеганография [Електронний ресурс] / Режим доступу: https://cryptowiki.net/index.php?title=Стеганография
22. Можно так просто взять и скрыть информацию [Електронний ресурс] / Режим доступу: https://habrahabr.ru/post/166583/
23. Конахович Г.Ф., Пузиренко А.Ю. Комп'ютерна стеганографія. Теорія та практика. [Текст] / Конахович Г.Ф.// Київ: МК-Пресс., 2006 р. – 288 с.
24. Cox I.J., Miller M., Bloom J., Fridrich J., Kalker T. Digital watermarking and steganography. [Текст] / Morgan Kaufmann, 2007 p. – 593 c.
25. Cvejic N. Algorithms for audio watermarking and steganography. [Текст] / Academic dissertation, Department of Electrical and Information Engineering, Information Processing Laboratory // University of Oulu, 2004 p. – 111 c.
26. Задирака В.К., Игисинов К. Анализ погрешности округления алгоритма быстрого преобразования Фурье и некоторых его приложений для режима с плавающей запятой [Текст] / Задирака В.К. // Киев, 1972 р. (Препр. Ин-т кибернетики им. В.М. Глушкова АН УССР: 72-23). – 593 с.
27. Задирака В.К. О сравнении некоторых алгоритмов вычисления оценок интеграла Фурье в корреляционной функции [Текст] / Математическое обеспечение ЭЦВМ // Киев: Ин-т кибернетики им. В.М. Глушкова АН УССР, 1971 р. – 249-250 с.
28. Задирака В.К. Цифровая обработка сигналов. [Текст] / Задирака В.К. // Киев: Наук. думка., 1993 р. – 294 с.
29. Задірака В.К., Кудін А.М., Людвіченко В.О., Олексюк О.С. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях [Текст]: / Задірака В.К. // Навч. Пос. – Київ—Тернопіль: Підручники і посібники, 2007 р. – 272 с.
30. Кошкина Н.В. Метод выделения инварианта к сдвигу, повороту и масштабированию для построения систем с ЦВЗ / Н.В. Кошкина, О.Ю. Никитина // Праці міжнар. конф. "Питання оптимізації обчислень-XXXIII". – Київ: Ін-т кібернетики ім. В.М. Глушкова НАН України. – 2007. – С. 142–143.

31. Zadiraka V. Spectral methods of computer steganography problem decision / V. Zadiraka, N. Koshkina // Methods of effective protection of information flows /ed. by V. Zadiraka, Y. Nykolaichuk. – Ternopil: Terno-graf, 2014. – P. 96–120.
32. Поліновський В.В. Інформаційна технологія для досліджень методів стеганографії і стеганоаналізу / В.В. Поліновський, В.Ю. Корольов, В.А. Гераси-менко, М.Л. Гоpинштейн // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – 2011. – №5. – С. 236–242.
33. Кошкіна Н.В. До питання часо-частотного аналізу сигналів в задачах комп'ютерної стеганографії / Н.В. Кошкіна // Праці міжнар. конф. "Питання оптимізації обчислень-XXXVI. – Київ: Ін-т кібернетики ім. В.М. Глушкова НАН України. – 2011. – Том 1. – С. 351–355.
34. Вовк О.О. Сравнительный анализ устойчивости к атакам стеганографи- ческих методов скрытия информации / О.О. Вовк, А.А. Астраханцев // Мат. 9-й Межд. мол. научно-техн. конф. «Современные проблемы радиотехники и телекоммуникаций РТ-2013». – 2013. – с. 153.
35. Кошкіна Н.В. Захист майнових прав на цифрову музику за допомогою стеганографічної технології «відбитків пальців» / Н.В. Кошкіна, Р.Г. Супроткін // Зб. мат. проблемно-наукової міжгал. конф. "Юриспруденція та проблеми інформаційного суспільства - 2011". – Івано-Франківськ. – 2011. – С. 110–111.
36. Кошкина Н.В. Внедрение ЦВЗ в аудиосигналы на основе пакетной вейвлет-декомпозиции и частотного маскирования / Н.В. Кошкина // Искусственный интеллект. – 2010. – № 4. – С. 381–387.
37. Мелешко Е.В. Метод встраивания двухуровневых цифровых водяных знаков в медиафайлы для защиты авторских прав / Е.В. Мелешко // Збірник на- укових праць Харківського університету Повітряних Сил. – 2013. – № 4. – С. 127-131.
38. Кошкина Н.В. Стеганоанализ бесключевых стеганосистем на основе атаки контрольным внедрением / Н.В. Кошкина // Междунар. научно-техн. журнал «Проблемы управления и информатики». – 2014. – № 6. – С. 137–144.

39. Liu Y. A novel audio steganalysis based on higher-order statistics of a distortion measure with Hausdorff distance / Y. Liu, K. Chiang, C. Corbett, R. Archibald, B. Mukherjee, D. Ghosal // Lecture Notes in Computer Science. – 2008. – № 5222. – P. 487 –501.
40. Кошкина Н.В. Исследование применимости матрицы смежности для выявления стеганоаудиоконтейнеров / Н.В. Кошкина // Междунар. научно-техн. журнал «Проблемы управления и информатики». – 2014. – №1 – С. 148–156.
41. Abolghasemi M. LSB data hiding detection based on gray level co-occurrence matrix / M. Abolghasemi, H. Aghainia, K. Faez, M.A. Mehrabi // International symposium on Telecommunications. – 2008. – P. 656–659.
42. Кошкіна Н.В. Методи стеганоаналізу з навчанням та класифікацією за характеристичними векторами / Н.В. Кошкіна // Праці міжнар. конф. “Питання оптимізації обчислень-XL”. – Київ: Ін-т кібернетики ім. В.М. Глушкова НАН України. – 2015. – С. 153–154.
43. Кошкина Н.В. Стеганография: выделение инварианта для процесса печати и сканирования / Н.В. Кошкина, О.Ю. Никитина // Мат. Второй межд. науч. конф. по проблемам безопасности и противодействия терроризму, М. –МГУ. – 2006. – С.304–307.
44. Задирака В.К. Статистический анализ систем с цифровыми водяными знаками / В.К. Задирака, Н.В. Кошкина, Л.Л. Никитенко // Искусственный интеллект.– 2008.– № 3. – С. 315–324
45. Wu C.-P. Robust and efficient digital audio watermarking using audio content analysis / C.-P. Wu, P.-C. Su, C.-C.J. Kuo // Proc. of SPIE Electronic Imaging, Security and Watermarking of Multimedia Contents II. – 2000. – Vol. 3971. – P. 382–392.
46. Wu C.-P. Robust audio watermarking for copyright protection / C.-P. Wu, P.- C. Su, K.C.-C. Jay // Proceedings of SPIE, Advanced Signal Processing Algorithms, Architectures, and Implementations IX. – 1999.– Vol. 3807. – P. 387–397.

47. Кошкина Н.В. Внедрение ЦВЗ в аудиосигналы на основе пакетной вейвлет-декомпозиции и частотного маскирования / Н.В. Кошкина // Искус- ственный интеллект. – 2010. – № 4. – С. 381–387.
48. Кошкіна Н.В. Новий метод цифрових водяних знаків для аудіосигналів / Н.В. Кошкіна // Матеріали 1 Міжнар. наук.-техн. конф. «Захист інформації і безпека інформаційних систем». – Львів. – 2012. – 120–121.
49. Xiang S. Robust Audio Watermarking Against the D/A and A/D conversions [Електронний ресурс] / S. Xiang, J. Huang. – 2007. – 29 p. – Режим доступу: http://arxiv.org/ftp/arxiv/papers/0707/0707.0397.pdf.
50. Термінологічний довідник з питань технічного захисту інформації / В. О. Хорошко, І. М. Огаркова, Д. В. Чирков та ін. ; за ред. проф. Хорошка В. О. – 3-тє вид., доп. і перероб. – К. : ТОВ "ПоліграфКонсалтинг", 2003. – 286 с.
51. Оков И. Н. О требуемой пропускной способности каналов передачи аутентифицированных сообщений в безусловно стойких системах / И. Н. Оков // Проблемы информационной безопасности. Компьютерные системы. – 2000. – № 3(7). – С. 78–64.
52. Грибунин В. Г. Стеганографическая защита речевых сигналов в каналах открытой телефонной связи / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев // Сборник тезисов Российской НТК "Методы и технические средства обеспечения безопасности информации". – СПб. : ГТУ, 2001. – С. 83–84.
53. A DWT-based technique for spatio-frequency masking of digital signatures / M. Barni, F. Bartolini, V. Cappellini, A. Lippi, A. Piva // Proceedings of the 11th SPIE Annual Symposium, Electronic Imaging '99, Security and Watermarking of Multimedia Contents. – 1999. – Vol. 3657.
54. Husrev T. Sencar. Data Hiding Fundamentals And Applications / Husrev T. Sencar, Mahalingam Ramkumar, Ali N. Akansu // Digital Multimedia. ELSEVIER science and technology books. – 2004. – 364 p.
55. Westfeld A. Attacks on Steganographic Systems. Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools – and Some Leassons Learned / A. Westfeld, A. Pfitzmann // Proceeding of the Workshop on Information Hiding. – 1999.

56. Ru X. Audio steganalysis based on “negative resonance phenomenon” caused by steganographic tools / X. Ru, Y. Zhuang, F. Wu // Journal of Zhejiang University SCIENCE A. – 2006. – Vol.7, № 4. – P. 577–583.
57. Geetha S. Audio steganalysis with Hausdorff distance higher order statistics using a rule based decision tree paradigm / S. Geetha, N. Ishwarya, N. Kamaraj // Expert system with applications journal. – 2010. – Vol. 37, № 12. – P. 7469–7482.
58. Niimi M. An attack to BPCS-steganography using complexity histogram and countermeasure / M. Niimi, T. Ei, H. Noda, E. Kawaguchi, B. Segee // Proc. International Conf. on Image Processing, ICIP. – 2004. – Vol.5. – P.733–736.
59. Поліновський В.В. Інформаційна технологія для досліджень методів стеганографії і стеганоаналізу / В.В. Поліновський, В.Ю. Корольов, В.А. Гераси-менко, М.Л. Горинштейн // Комп’ютерно-інтегровані технології: освіта, наука, виробництво. – 2011. – №5. – С. 236–242.
60. Yang S. Quantization-Based Digital Audio Watermar-king in Discrete Fourier Transform Domain / S. Yang, W. Tan, Y. Chen, W. Ma // Journal of Multimedia. – 2010. – Vol. 5, № 2. – P. 151–158.
61. Perez-Freire L. Watermarking security: a survey / L. Perez-Freire, P. Comesana, J.R. Troncoso-Pastoriza, F. Perez-Gonzalez // Transactions on Data Hiding and Multimedia Security, 2006. – Vol. 4300. – P. 41–72.
62. Кудин А.М. Математическая модель стеганографической системы на базе общей теории оптимальных алгоритмов/ А.М. Кудин // Математичне та комп’ютерне моделювання. Серія: Технічні науки. – 2010. – Вип. 4. – С. 136 – 143.
63. Кошкина Н.В. Спектральные методы решения задач компьютерной стеганографии / Н.В. Кошкина, В.К. Задирака // Междунар. научно-техн. журнал «Проблемы управления и информатики». – 2011. – №4. – С. 132–151.
64. Farid H. Detecting hidden messages using higher-order statistical models / H. Farid // Proc. of the Intl. Conf. on Image Processing. IEEE. – 2002. – Vol.2. – P. 905–908.
65. Ахмад Х.М. Введение в цифровую обработку речевых сигналов / Х.М. Ахмад, В.Ф. Жирков. – Владимир: Изд-во Владим. гос. ун-та, 2007. – 192 с.

66. Кошкина Н.В. Стеганоанализ бесключевых стеганосистем на основе атаки контрольным внедрением / Н.В. Кошкина // Междунар. научно-техн. журнал «Проблемы управления и информатики». – 2014. – № 6. – С. 137–144.
67. Капуста А.М. Методы статистической классификации в задаче обнаружения встраивания информации / А.М. Капуста // Сб. работ 68-й науч. конф. студентов и аспирантов Белорусского гос. ун-та 16-19 мая 2011 г.: в 3-х ч.: ч. 1. – Минск, 2011. – С. 117–120
68.. Вовк О.О. Сравнительный анализ устойчивости к атакам стеганографических методов скрытия информации / О.О. Вовк, А.А. Астраханцев // Мат. 9-й Межд. мол. научно-техн. конф. «Современные проблемы радиотехники и телекоммуникаций РТ-2013». – 2013. – с. 153.
69. Задирака В.К. К вопросу стойкости стеганосистемы при пассивных атаках / В.К. Задирака, Л.Л. Никитенко // Междунар. научно-техн. журнал «Проблемы управления и информатики». – 2009. – № 2. – С. 138 – 139.

ДОДАТОК А ГРАФІЧНИЙ МАТЕРІАЛ

ПЛАКАТ 1 Діаграма діяльності

ПЛАКАТ 2 Діаграма варіантів використання

ПЛАКАТ 3 Діаграма послідовності

ПЛАКАТ 4 Екранні форми

ПЛАКАТ 5 Екранні форми

ПЛАКАТ 6 Результати дослідження

ПЛАКАТ 7 Результати дослідження